NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

LEVERAGING THE NATIONAL GUARD'S EXISTING INFORMATION TECHNOLOGY INFRASTRUCTURE TO BRIDGE THE INCIDENT RESPONSE DIGITAL DIVIDE

by

Stephan Picard

September 2004

Thesis Advisor: William J. Welch
Second Reader: Maureen Lischke

Approved for public release; distribution is unlimited

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE			Form Approved OMB No. 0704-0188
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington DC 20503.			
1. AGENCY USE ONLY *(Leave blank)*	**2. REPORT DATE** September 2004	**3. REPORT TYPE AND DATES COVERED** Master's Thesis	
4. TITLE AND SUBTITLE: Leveraging the National Guard's Existing Information Technology Infrastructure to Bridge the Incident Response Digital Divide		**5. FUNDING NUMBERS**	
6. AUTHOR(S) Stephan Picard			
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000		**8. PERFORMING ORGANIZATION REPORT NUMBER**	
9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A		**10. SPONSORING/MONITORING AGENCY REPORT NUMBER**	
11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.			
12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release; distribution is unlimited		**12b. DISTRIBUTION CODE** A	

13. ABSTRACT (maximum 200 words)

One of the greatest challenges facing the United States after a concerted terrorist attack is that of coordinating response from the myriad of resources available to the incident commander. During this crisis, the daunting task facing the Information Technology (IT) community is to bring a myriad of disparate systems and their relevant traffic together to provide the incident commander a picture of what is happening on the ground, a common operating picture, and then to push that picture up to the decision makers at the state and federal levels.

This thesis will examine current organizational structures, missions and IT architectures within the United States Department of Homeland Security, United States Northern Command and the United States National Guard. In addition, this thesis will propose that one solution to bridge the divide between the disparate agencies that may respond to an emergency such as a natural disaster or a terrorist Weapon of Mass Destruction (WMD) may lie within the National Guard. With its unique role as a state militia and a federal warfighter, the National Guard is particularly well positioned to bridge this divide by augmenting its existing networks and incident response communications capabilities.

14. SUBJECT TERMS National Guard, Incident Response, Homeland Security, Homeland Defense, Communications, Infrastructure, September 11, 2001			**15. NUMBER OF PAGES** 109
			16. PRICE CODE
17. SECURITY CLASSIFICATION OF REPORT Unclassified	**18. SECURITY CLASSIFICATION OF THIS PAGE** Unclassified	**19. SECURITY CLASSIFICATION OF ABSTRACT** Unclassified	**20. LIMITATION OF ABSTRACT** UL

NSN 7540-01-280-5500

Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. 239-18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release; distribution is unlimited

LEVERAGING THE NATIONAL GUARD'S EXISTING INFORMATION TECHNOLOGY INFRASTRUCTURE TO BRIDGE THE INCIDENT RESPONSE DIGITAL DIVIDE

Stephan J. Picard
Major, United States Army
B.S., Eastern Connecticut State University, 1992

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN SYSTEMS ENGINEERING

from the

NAVAL POSTGRADUATE SCHOOL
September 2004

Author: Stephan Picard

Approved by: Professor William J. Welch
Thesis Advisor

Ms. Maureen Lischke
Second Reader

Phil DePoy, Ph.D.
Director, Wayne E. Meyer Institute of Systems Engineering

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

One of the greatest challenges facing the United States after a concerted terrorist attack is that of coordinating response from the myriad of resources available to the incident commander. During this crisis, the daunting task facing the Information Technology (IT) community is to bring a myriad of disparate systems and their relevant traffic together to provide the incident commander a picture of what is happening on the ground, a common operating picture, and then to push that picture up to the decision makers at the state and federal levels.

This thesis will examine current organizational structures, missions and IT architectures within the United States Department of Homeland Security, United States Northern Command and the United States National Guard. In addition, this thesis will propose that one solution to bridge the divide between the disparate agencies that may respond to an emergency such as a natural disaster or a terrorist Weapon of Mass Destruction (WMD) may lie within the National Guard. With its unique role as a state militia and a federal warfighter, the National Guard is particularly well positioned to bridge this divide by augmenting its existing networks and incident response communications capabilities.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

LIST OF FIGURES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF TABLES

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGMENTS

I am deeply grateful to Ms. Maureen Lischke, the CIO of the National Guard Bureau, for her leadership and mentorship that became the foundation for the development of this thesis. Ms. Lischke is truly a visionary who sees the good that information technology can bring to the world. Ms. Lischke understands that the capabilities of communication, collaboration and information synthesis do not exist simply to exist, but to respond to the needs of the user.

I would also like to thank Ms. Kathy Pritchett, the Chief of the Joint IT Programs Branch, NGB-J6, for her generosity and understanding as I undertook this endeavor.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

Many of the communication issues that exist today within the community that responds to the United States' emergencies have existed for years. The events of September 11, 2001 (9-11) demonstrated that our communications systems, while powerful and far reaching, do not always have the capability to communicate amongst themselves. More importantly, the events of 9-11 gave our Nation a sense of urgency in solving these issues. To have one of the world's most advanced communications systems, but not be able to communicate at the incident site, disturbs our moral conscience and on 9-11 many lives within the first responder community were lost due to communications equipment that could not deliver vital messages about the imminent collapse of the towers to all involved. In this instance, the different agencies responding to the crisis were able to share information amongst their own group, but not with others. During the early hours after the first aircraft crashed into the twin towers, the Mayor could not effectively communicate with the on-scene police and fire department commanders due to disparate radio networks. This deficiency became even more acute as the system provided to the fire department could not communicate the imminent collapse of the towers to the fire personnel that were inside the buildings, while the police warnings to their personnel got through. The lack of interoperability between those two FM communications systems led to dozens if not hundreds of deaths.

It is recognized at all levels within the United States government that Information Technology (IT) has an important role to play in securing our homeland and there is no shortage of resources. In Fiscal Year 2003, the President's budget for government wide IT was 56.1 billion dollars. (GAO Report on Homeland Security Funding and Management Issues, 2002, p. 12) The General Accounting Office (GAO) identified four specific roles that IT has in securing the homeland in their report to Congress on Homeland Security IT funding and management. In the report, the GAO stated,

> Information technology (IT) will play a critical role in strengthening our nation's homeland security against potential future attacks. Specifically, IT will help enable the nation to identify potential threats, share information more readily, provide mechanisms to protect our homeland, and develop response capabilities. (GAO Report on Homeland Security Funding and Management Issues, 2002, p. 2)

In August of 2003, the GAO reported that with regard to current information and intelligence sharing processes, state and local agencies

> identified three systemic problems. First, they believe that needed information is not routinely provided. Second, the information that they do receive is not always timely, accurate, or relevant. Third, they feel that the federal government still perceives the fight against terrorism to be generally a federal responsibility and consequently does not integrate state and city governments into the information-sharing process. (GAO Report, Homeland Security, Efforts to Improve Information Sharing Need to be Strengthened, 2003, p. 20)

The digital divide at the incident response site has been created as IT falls short of its role in securing the homeland. This is due to its failure to provide timely, accurate and relevant data at the right place and at the right time.

The investment required to replace the communications infrastructure in the United States simply is too large for us to undertake. It is essential that some agency be tasked to respond to the scene of a disaster and bring with it not only the technical capability to bridge the communications divide between local, state and federal responders, but also the legal capability. This thesis will examine current organizational structures, missions, and IT architectures within the Department of Homeland Security, Northern Command, and the National Guard and provide one of many potential solutions to help bridge the divide between the disparate agencies that may respond to an emergency such as a natural disaster or a terrorist Weapon of Mass Destruction (WMD). This thesis proposes that the National Guard, with its unique role as a state militia and a federal warfighter, is uniquely positioned to fulfill this mission by augmenting its existing IT infrastructure and personnel, bridging the incident response digital divide.

II. LOCAL INCIDENT RESPONSE

To study how best to support the local community and its first responders, it is important to first understand the situation at the incident site and how the local governments operate. In a report issued in August of 2003, the GAO found that,

> Since September 11, 2001, federal, state, and city governments have established initiatives to improve the sharing of information to prevent terrorism. Many of these initiatives were implemented by states and cities and not necessarily coordinated with other sharing initiatives, including those by federal agencies. At the same time, the Department of Homeland Security (DHS) has initiatives under way to enhance information sharing, including the development of a homeland security blueprint, known as an "enterprise architecture," to integrate sharing between federal, state, and city authorities. (GAO Report, Homeland Security, Efforts to Improve Information Sharing Need to be Strengthened, 2003, p. 2)

In a democratic open society such as the United States, it is inevitable that every state, city and local municipality will be different leading to disparate communications networks servicing different governmental agencies. In some municipalities there is a central figure, such as the Mayor of New York, who is in command of the incident response on the local level and all city agencies report to him, while in some municipalities, there is no central figure other than a sheriff or a constable who must build a response from agencies not under their control. This very fact is one of the key issues facing a unified response to any incident site in support of the local responders. It is extremely difficult to build a standard operating procedure for response when the situation at the incident site can be extremely diverse. No matter what type of local governmental system is in place, there remains the need to communicate horizontally within the response agencies and vertically from the incident to the incident commander and above to state and federal levels.

A. THE EMERGENCY OPERATIONS CENTER

In most local responses, the 911 emergency networks direct the initial allocation of resources to support the incident. This network will dispatch field units, initiate and transfer calls to other dispatch centers, and notify the state or county Emergency Operations Center (EOC) if necessary. Much of the incident response is based upon predetermined criteria and can be extremely difficult to coordinate. This is due to the fact that a significant portion of the county-wide response is at times made up of non-county responders such as state police, military, federal, state and city agencies to include non-governmental organizations such as the Red Cross and private industry such as the local utilities. (Scott, 2003, p. 64) Typically, the EOC of a jurisdiction is not fully manned 24 hours a day, and only becomes so in response to a particular incident. According to Scott in his thesis,

> When activated the EOC is typically staffed with representatives, but not directors of the various county agencies, other governments and NGO's. The "Commander" of the EOC controls the operations of the EOC itself, but often does not have the authority to direct the response provided by an agency represented at the EOC….the EOC serves as a focal point for cooperation between the county and the non-county government agencies that might be affected by the crisis, including cities within the county, federal facilities located within the county, neighboring EOC and the…state EOC (Scott, 2003, p. 65)

The infrastructure that supports the local EOC is as varied as the make up of the counties and cities themselves, but the typical EOC is similar to the Monterey EOC that Scott studied in his thesis. In Monterey, the prime communications method the members of the EOC staff use to communicate with their agencies is the telephone. There are a number of shared computer workstations that provide connection to the Internet, email for each of the established EOC positions and a number of Local Area Network (LAN) drops for those members who have laptop computers. The EOC utilizes voice-only satellite radio and high frequency 150 MHz radios as its backup in case the public switched telephone service is disrupted. In addition, it has a number of software systems, the Response Information Management System (RIMS) and

the Emergency Digital Information System (EDIS), to publish text message traffic throughout the state. Communications with the responders at the incident site are provided by cell phone and radio. (Scott, 2003, p. 68)

B. THE INCIDENT SITE

At the incident site, the incident commander is in charge. The agency fielding the incident commander is determined by the type of incident, the agencies available for response and the political environment within that jurisdiction. In most situations, the incident commander can control those agencies and assets that respond to the incident site, de-conflicting responses, but does not have the authority to requisition additional assets. The incident commander is not a leader in the military sense and the majority of decisions at the incident site will be made through consensus with the responding agencies. In the early hours of a severe crisis, this is a critical problem that can only be overcome through instant and accurate communications amongst all local, state, and federal agencies that have assets available to the incident commander. The incident commander must understand the situation at hand, what assets are available for their use, and how to access those assets.

The infrastructure at the incident site is far less capable and more varied than the infrastructure seen at the EOC and above. An example of this is in the way information is shared. While at the EOC, all parties sit within close proximity and computers fuse data for aggregated information flow, often the response assets are not integrated in order to provide a common operating picture at the incident. The primary means of communication at the incident site is hand-held radio and cell phone. Many of the agencies responding to the incident utilize their own particular band or frequency for said traffic and as such, cannot communicate horizontally in order to coordinate the response. This was evidenced in graphic detail in the response to 9-11 when the New York Police Department issued a warning that the towers were about to collapse and the New York Fire Department members could not and did not receive this warning. It is a fact that many lives were lost due to this lack of rudimentary capability.

The problem expressed in this section has three facets. First, how can we bridge the communications gap at the incident site in order to coordinate and manage response? Second, how can we bridge the communications gap at the EOC level and higher to efficiently manage resources and provide the incident commander with the appropriate mix of responses at the appropriate time and at the appropriate place? Lastly, how can we mine the information from multiple incident sites and EOCs, bridging the communications gap and providing a common operating picture at all levels of government from the Governor to the President, in order to have an understanding of the entire scenario that may be unfolding? In the following sections, I will try to provide an understanding of the federal players in this arena, the National Guard, United States Northern Command (USNORTHCOM) and the Department of Homeland Security (DHS), showing the unique position of the National Guard and its IT infrastructure in bridging the incident response digital divide.

III. THE UNITED STATES NATIONAL GUARD

The National Guard, consisting of fifty-four state and territorial entities (i.e., Guam National Guard), principally serves under the command of the relevant state or territorial Governor for missions including response to civil disorder and natural disasters. When federalized for combat or national security missions, however, each State National Guard serves under the command of the President. Thus, sometimes the Guard's homeland security mission will be determined at the state and territorial level and, at other times, at the federal level.

A. THE CONNECTICUT STATE MILITIA

In order to better understand how the National Guard relates to the local communities and how it is postured in this ever changing environment to serve as the bridge between the local, state and federal response during time of disaster, it is important to understand its lineage. In an attempt to explain this lineage and its ties to the community, I will present the Connecticut State Militia as a case study of how the National Guard was formed beginning in 1636.

The 17th Century was a time of war between the settlers of what is now Connecticut and the American Indian Pequot nation. (Walsh, 1991, p.6) In 1636, the Pequots attacked the Dutch settlement at Saybrook and skirmished as far north as Wethersfield, forcing the settlers to form the first community based militia. On May 15, 1636, John Mason, a captain in the British "trainband"[1] tradition, was ordered by the General Court to raise men from the communities of Hartford, Windsor and Wethersfield to counter the Pequot threat. (Walsh, 1991, p. 9) The method of this group's formation is the very foundation of how today's National Guard is built. In 1636, Mason sailed down the Connecticut River and formed the first Connecticut Militia with volunteers from the communities and

[1] "trainband" The term draws its roots from an English tradition in which the English Militia was formed by a trained band of men whose instruments were that of war, not music. (Walsh, 1991, p. 6)

fielded this group as town militia companies rather than as units comprised of individuals from disparate locations. This tradition can still be found in many National Guard units today.

In March of 1637, Mason was titled "*publique military officer of the plantacions of Connecticut*" (Walsh, 1991, p. 10) by the General Court. In addition, the Court established the roots of today's National Guard "drill" and "Annual Training (AT)"[2] by ordering that *a magazine of shot and powder be established in four communities and that all men aged sixteen to sixty bear arms and attend ten days of training annually.* (Walsh, 1991, p. 10)

As stated earlier, these militia bands were organized by town, but on June 26, 1672 the regimental system was adopted to better serve the colony as a whole. (Walsh, 1991, p.12) These regiments, formed in 1672 as the Regiments of Hartford, New Haven and Fairfield Counties, continue with unbroken service in today's National Guard as the 169th Infantry Regiment, the 102 Infantry Regiment and the 192 Field Artillery Regiment, respectively.

The origination of the National Guard within the United States began at the founding of our country. Article I, Section Eight of the Constitution states,

> Congress shall have power to lay and collect taxes, duties, imposts and excises, to pay the debts and provide for the common defense and general welfare of the United States; …To raise and support armies, but no appropriation of money shall be for a term longer than two years; …To provide for the calling forth the militia to execute the laws of the union, suppress insurrections and repel invasions; to provide for organizing, arming and disciplining, the militia, and for governing such part of them as may be employed in the service of the United States, reserving to the states respectively, the appointment of the officers, and the authority of training the militia according to the discipline prescribed by Congress. (US Constitution, Article I, Section 8)

There are two points within this excerpt that are especially critical to understanding the dual role of the National Guard. The first is that though the Congress has the right to call forth the militia, it reserves "*to the states*

[2] "Drill", "Annual Training" Today's National Guard "drills" one weekend a month and performs two weeks of Annual Training a year.

respectively" the day to day operation and training of the National Guard, and the appointment of its officers. These two points are still true to this day and shape how the National Guard interacts within the United States on multiple levels.

In 1916, the National Defense Act changed the State Militias from a state based force to the "principal" reserve component for the United States Army and made mandatory the title for the reserve component the "National Guard" (Van Fleet, 2002, p.10)

The National Guard as it stands today has a proud history and foundation in its communities. It is made up of soldiers and airmen that perform their military duties during "drills" much as the militiamen in 1636 did. When these soldiers and airmen are not in uniform, they are the community; they are the people who make up the local, state and federal levels. There is much made about the interface between these levels of government and community in time of crisis. In his thesis conclusion, Edward Lockwood makes the point that,

> …the Army National Guard's unique ability to reach and harness the power of American communities is a national asset. It provides the ability to use the best America has to offer and our national spirit of volunteerism. It is an untapped resource that when managed correctly demonstrates the best in civil-military relations and civilian control of the military. (Lockwood, 2003, p. 64)

In the Reserve Component Employment Study (RCES) of 2005, the Assistant Secretary of Defense for Strategy and Threat Reduction stated,

> The Reserve Component (RC) are dispersed regionally throughout the nation, are populated with community residents, and have established ties with local authorities. These unique characteristics make them prime candidates for supporting missions such as assisting civil agencies in the management of the consequences of a WMD attack (WMD CM) or providing physical security for critical assets such as key infrastructure nodes. (Under Secretary of Defense for Strategy and Threat Reduction, 2004, p. 66)

The National Guard and its unique mix of community based participants are poised to take a leading role protecting the Homeland.

B. TITLE 10, TITLE 32, STATE ACTIVE DUTY

The National Defense Act of 1933 is the most important piece of this legislation and that which is most germane to this thesis and to the National Guard's role in homeland security and homeland defense. The National Defense Act of 1933 established the two identities of the National Guard; it established the National Guard of the United States and the National Guard of the Several States. The National Guard of the United States is the National Guard that is a deployable asset for the Active Army and Air Force, Title 10 United States Code (USC), and the National Guard of the Several States is the State Militia, Title 32 USC, which is deployable by the Governor in response to State emergency. (Van Fleet, 2002, p. 10) According to Edward Lockwood in his thesis,

> The 1933 amendments to the National Defense Act of 1920 provided the legal basis for the State National Guard entities to become the Army National Guard of the United States when federally mobilized. In essence, the 1933 amendments recognized the dual nature of the Army National Guard as a state and federal entity, a kind of dual citizenship in the profession of arms. (Lockwood, 2003, p. 39)

He goes on to say that,

> In recognizing that the Army National Guard is a reserve of the Army, the Army created a situation by which the Army National Guard units could mobilize as units and deploy overseas in support of the foreign policy of the United States. (Lockwood, 2003, p. 39)

The National Guard, through its dual missions, can and does bridge the gap between state and federal levels on a regular basis, whereas most state and federal agencies are just that, state or federal. This unique ability is stated very clearly in the 2005 National Guard Posture Statement:

> The Guard was there when it was needed, demonstrating the flexible accessibility inherent in the unique multi-status roles of the Guard. Our Homeland Defense and Security roles mandate that we be capable of seamlessly operating in federal and state intergovernmental and interagency roles. September 11th and its aftermath are illustrative of the Guard's new operating environment and its unique flexibility to respond to our nations needs. (NGB, 2005 National Guard Posture Statement, 2004, p. 1)

The days and months following September 11th illustrate a specific case whereby the advantage of a dual role National Guard was demonstrated. Four days after the attack, the President of the United States determined that it was essential to re-open the nation's commercial airports that had been shut down since 9-11. To provide additional security and a sense of comfort to the American public, the President decided to emplace military forces in the airports. The Posse Comitatus Act of 1878 states that,

> Whoever, except in cases and under circumstances expressly authorized by the Constitution or Act of Congress, willfully uses any part of the Army or the Air Force as a posse comitatus or otherwise to execute the laws shall be fined under this title or imprisoned not more than two years, or both. (US Code Collection, 2004, p. 1)

Therefore, it is forbidden to utilize the federal military to perform law enforcement missions such as airport security. Leveraging the dual role of the National Guard, the President called upon the Governors to activate the National Guard under Title 32 for the airport security mission. This mission was performed in Title 32 status until its conclusion a year later.

In addition to the two identities established by the 1933 amendments to the Defense Act of 1920, there exists a third identity for the National Guard. The Governors in accordance with the laws of their particular State may activate their National Guard under State Active Duty to fulfill a State mission. Under this particular identity, the National Guard is paid directly from the State coffers and is under the command of the Governor.

C. THE NATIONAL GUARD BUREAU

In 1916, the National Defense Act restructured the division of Militia Affairs into a separate Militia Bureau and assigned two full-time National Guard officers to the Militia Bureau that had, as the Division of Militia Affairs, been staffed with Regular Army officers. In January 1921, an amendment to the National Defense Act stated that the Chief of the Militia Bureau would be selected from a list of National Guard officers. This billet had been a Regular Army billet up until this

point. The Chief of today's National Guard Bureau is nominated by the Governors of the states, appointed by the President and confirmed by the Senate. In 1933, The National Defense Act renamed the Militia Bureau to the National Guard Bureau (NGB) and established the National Guard as a reserve component. (Van Fleet, 2002, pp. 9-10)

The NGB serves to manage the federal funds utilized in the training and operation of the National Guard and is the official channel of communication from the respective service to the state or territorial National Guard as stated in Title 10, USC, Part I chapter 1011, Section 10501(b).

> …the channel of communications on all matters pertaining to the National Guard, the Army National Guard of the United States and the Air National Guard of the United States between the Department of Army and the Department of Air Force and the several States. (Title 10, USC, Part I chapter 1011, Section 10501(b))

According to the Chief of the National Guard Bureau (CNGB), Army Lieutenant General H. Steven Blum as he briefed the Joint Staff in April of 2004, the mission of the NGB is:

> To acquire, manage, and distribute Army and Air National Guard resources; to develop and administer policies and programs in support of the National Security Strategy; to act as the "Channel of Communications" between the Services and the National Guard of the States, Territories and the District of Columbia as well as other internal and external agencies for the successful accomplishment of CONUS and OCONUS missions. (NGB, NGvision Brief, 2004, p. 2)[3]

This mission statement hits upon both of the National Guard Bureau's missions and demonstrates the role that it plays. As stated in the previous section on the history of the National Guard, there are two National Guards, the National Guard of the United States (federal status) and the National Guard of the several States (state status). The NGB does not have any command relationships with either of these Guard structures. In federal status, the Guard members report through the active component to the President of the United States as Commander in Chief

[3] CONUS (Continental United States), OCONUS (Outside Continental United States)

and in state status, the Guard members report to their respective Governors. The National Guard Bureau is simply a channel of communications between the services and the states and a conduit for federal funds into the States. Lieutenant General H. Steven Blum, the current CNGB, demonstrates the significance of what the NGB does through his vision for the NGB, as stated in his vision brief.

> To "provide for the common defense"…of the nation, the National Guard Bureau provides the leadership and resources required to set the standard for the world's premier reserve force, the National Guard of the United States. Our destiny is to respond to current and future worldwide commitments of the National Security Strategy with community-based, dedicated, citizen-soldiers and airmen; well-trained, organized, and supported with state of the art technology and equipment. (NGB, NGvision Brief, 2004, p. 2)

1. Organization

In 2004, the National Guard Bureau was reorganized into a Joint Staff that closely mirrored that which exists within the DoD in the headquarters at the Pentagon. This staff was divided into eight main sections. A Memorandum from Major General Sullivan, the Director of the Joint Staff dictated that,

> The term "NGB Joint Staff" is defined as the J1 through J8 directorates, the Special Staff and Personal Staff elements. (Sullivan, 2004, p. 1)

Figure 1 (Sullivan, 2004, p. 2) details the Organizational Chart for the National Guard Bureau as outlined by Major General Sullivan.

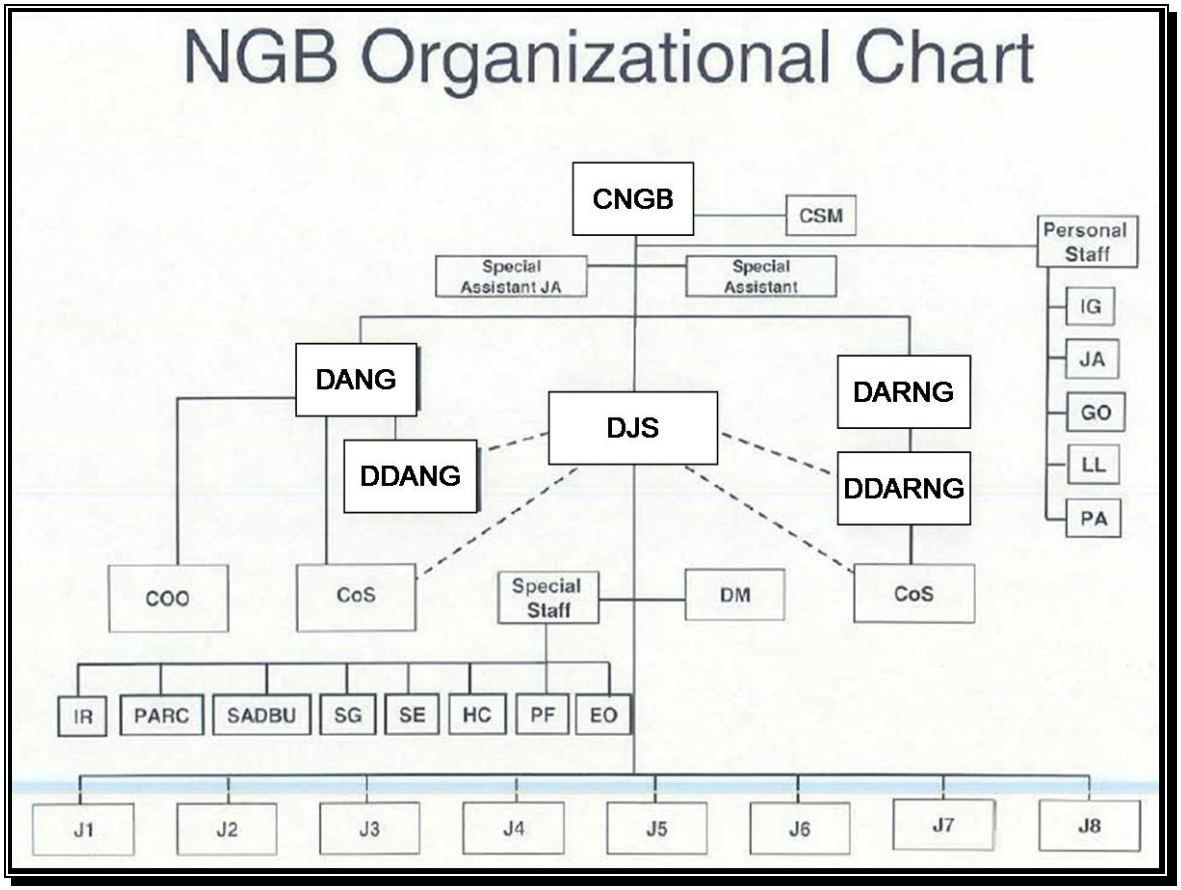

Figure 1. NGB Organization Chart

Much of this organization is the same as a typical Joint Staff, but there are two branches of the tree that are unique to the National Guard Bureau. These are the branches directly under the Chief of the National Guard (CNGB) and his special staff, that branch to the left and right. These branches lead to the Directors of the Army National Guard and the Air National Guard, Lieutenant General Schultz and Lieutenant General James. These two positions command their own staffs and work very closely with the parent services, the Army and the Air Force, in order to integrate the Guard into the total force. They are advisors to the CNGB on matters pertaining to their respective service and work very closely with the Director of the Joint Staff. The NGB Joint Staff answers directly to the Director of the Joint Staff and ultimately to the CNGB, but does not answer

to the Director of the Army National Guard or the Director of the Air National Guard. In his memo, Major General Sullivan stated the mission of the Joint Staff as

> The Joint Staff assists the Chief, NGB in accomplishing his responsibilities for strategic direction of the National Guard Forces; their operation under unified command; and their integration into an efficient team of land and air forces. (Sullivan, 2004, p. 1)

A major change within the National Guard Bureau that occurred during this reorganization is the inclusion in the Joint Staff of both Navy and Marine Corps personnel on the staff. Prior to the reorganization, the staff was made up of only Army and Air Force personnel. The inclusion of Navy and Marine Corps personnel is intended to better round the staff and provide input to the CNGB from all components.

2. NGBJ6/CIO

To meet both its state and federal missions, the National Guard maintains an interconnected information technology infrastructure within and across the fifty-four states and territories. Most of the infrastructure, the wiring and the equipment, as well as the people, who manage and maintain it, are under the command of the relevant state or territorial Governor; some of the interconnecting infrastructure, however, is federally funded and controlled.

The Chief of the National Guard Bureau, LTG Blum, summarized well the role of the NGB-J6. He stated,

> I want you leveraging all the Army's systems and all the Air Systems to come up with the best purple systems ultimately. …We're going to lead from the rear. The Guard is actually going to push a much, much bigger DoD in the right direction. (Blum, 2003, p. 6)

The NGB J6's primary role is to do just what LTG Blum stated: to leverage Army and Air Guard IT systems in order to create a NGB enterprise system. As stated in the NGB IT Vision/Mission Brief, the mission of the NGB J6 is,

> To acquire, manage, and distribute Army and Air National Guard IT resources to develop and administer IT policies and programs in

> support of the National Security Strategy; to act as the "Channel of Communications" on IT issues between the Services and the National Guard of the States, Territories, and the District of Columbia as well as other internal and external agencies for the successful accomplishment of CONUS and OCONUS missions. (NGB, NGB IT Vision/Mission Brief, 2004, p. 2)

In order to support this mission, the National Guard has deployed a nationwide IT infrastructure. Figure 2 (NGB, JettCon Shared Usage Brief, 2001, p. 6) illustrates the multiple missions that the National Guard IT infrastructure supports. The NGB J6 must integrate all voice, video, and data into an enterprise wide solution that will support the missions of:

- Readiness: The "go-to war" mission. This includes all training and preparation in support of National Guard warfighting capabilities.
- Counterdrug: One of the National Guard's Military Assistance to Civilian Authorities (MACA) missions.
- Stability and Support: The National Guard's primary state mission, responding within the state in times of emergency and natural disaster.
- Shared Usage: A congressionally mandated mission to make the National Guard's Distributed Training Technology Program available to anyone on a space available, reimbursable basis.
- State Partnership Program: The National Guard mission partnering with friendly nations in partnership to facilitate education and training in support of national objectives.
- Family and Youth Programs: Programs like STARBASE and Youth ChalleNGe that work with disadvantaged youth in order to give them the skills required to succeed. Additionally, providing support to family members of deployed soldiers and airmen.

Figure 2. National Guard IT Missions

- Homeland Security: The National Guard's mission at home to secure the homeland and to respond to any terrorist incident such as 9-11.
- Information Operations/Assurance: The National Guard's mission to secure the electronic traffic that flows through the United States and to prevent disruptions to service and operations.

This integration of National Guard IT into an enterprise was recently recognized by LTG Blum in his speech to the Joint IT Conference. He stated that the NGB IT community must,

> …get the Air Warrior Net, and the GuardNet and RCAS to come together. So we have a much more powerful enterprise system. (Blum, 2003, p. 7)

In subsequent sections, this thesis will describe each of these National Guard systems and how they can serve to enhance homeland security and bridge the digital divide at the incident site.

3. GuardNet XXI

GuardNet XXI is a congressionally funded information network that currently features an Asynchronous Transfer Mode (ATM) backbone providing terrestrial and satellite connectivity to all 54 States, Territories and the District of Columbia into over 3300 Armories and Airbases. Figure 3 (RCAS Summary, 2004, p. 1) depicts the multiple Interfaces into GuardNet XXI that provide high speed information access in support of multiple missions.

Figure 3. GuardNet XXI connections

The Wide Area Network (WAN) that connects the National Guard's nationwide infrastructure, GuardNet XXI, consists of a hub and spoke architecture with seven major hubs located in the states of Virginia, North Carolina, Iowa, California, Wyoming, Arkansas and New York and provides

telecommunications through a Dual DS3[4] backbone with a minimum of a T1[5] connection into each State and Territory as illustrated in Figure 4. (NGB, JettCon Shared Usage Brief, 2001, p. 8) Currently, the circuits that make up GuardNet XXI are leased through the Federal Telecommunications System (FTS) 2001 contract and are provided by MCI. GuardNet XXI is an unclassified network that is accredited at the level of Sensitive But Unclassified (SBU).

Figure 4. GuardNet XXI current configuration

At this writing, GuardNet XXI is undergoing a modernization project in order to capitalize on new technology and to provide significant increases in bandwidth, security, flexibility and redundancy. In October 2004, the projected completion date of the modernization, GuardNet XXI will have changed from the current ATM architecture of hub and spoke to Sprint's peerless Internet Protocol (IP) network pictured in Figure 5. (NGB, NGB Brief Kickoff, 2003, p. 7) As of July of 2004, this modernization project was on schedule.

[4] DS3 circuit provides 45 million bits per second (Mbps) of throughput.

[5] T1 Circuit provides 1.54 Mbps throughput.

This network will be leased from Sprint and will increase the amount of bandwidth available to the National Guard for its missions and those of its federal, state and local partners from 45 Mbps to 155 Mbps. The Sprint network allows for dynamic routing which will allow any connection to be routed over the best, least congested path from origination to destination. This will reduce the number of hops traffic will be required to take in order to arrive at its destination.

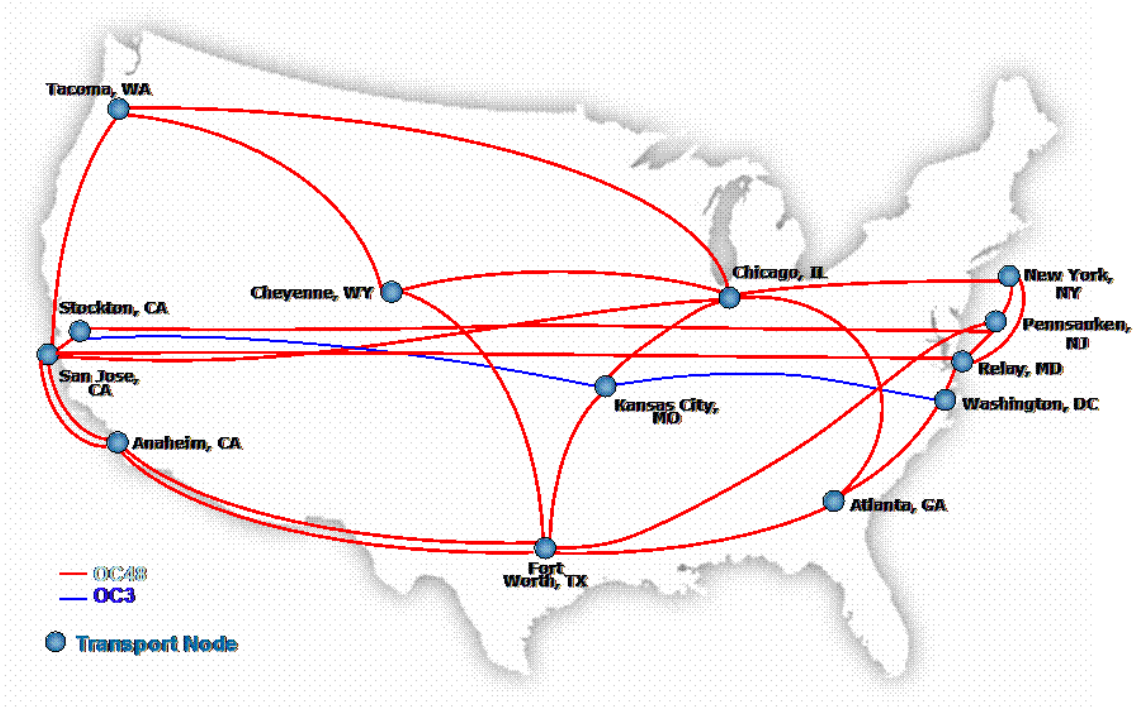

Figure 5. Sprint Peerless IP Network[6]

This architecture eliminates the single points of failure that currently exist in the ATM design by allowing the network to reroute traffic dynamically in response to changing conditions. In this design, no one device failure can or will bring down the network. Figure 6 (NGB, NGB Brief Kickoff, 2003, p. 11) shows the new architecture for GuardNet XXI and demonstrates the multiple paths through Sprint's network that can be utilized if one arc goes down. Another significant change to GuardNet XXI is the conversion of the backbone from ATM to IP. This change required significant change to the National Guard's Distance Learning (DL) program, the Distributive Training Technology Project (DTTP), which will be

[6]OC3 provides 155 Mbps throughput and an OC98 provides 9000 Mbps or 9 Gbps throughput.

discussed in the DTTP section. The previous design was constructed mainly to support ATM video teleconferences (VTC) and required transcoding of all IP traffic from IP to ATM at the nearest hub in order to transit the network, then transcoding it back to IP at the destination hub. This can cause significant latency and causes increased cost and complexity. Since the advent of IP VTC, it is now possible to combine all traffic on one network utilizing Virtual Private Networks (VPN) and avoid the necessity of transcoding traffic.

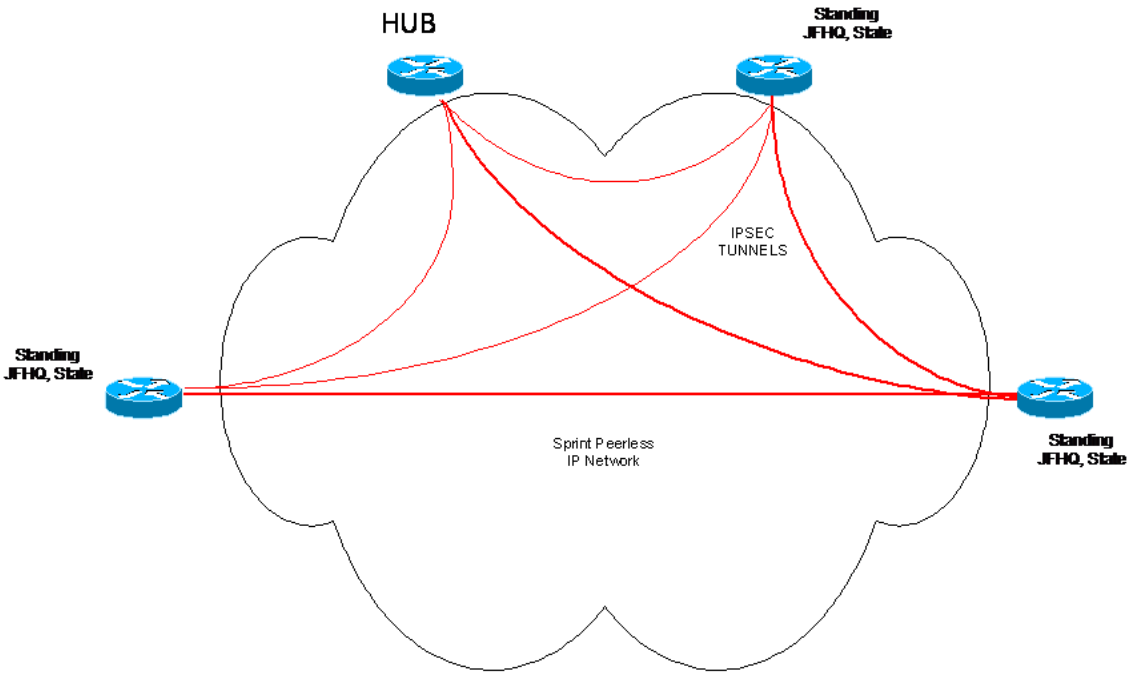

Figure 6. GuardNet XXI Meshed IP Virtual Network Tunnels

The new GuardNet XXI architecture also provides for additional security from the previous design. Sprint's peerless IP network is a private IP backbone where the National Guard will have its own dedicated fiber in order to carry its traffic. This private network is physically removed from the public switch network where the Internet resides, unlike the current architecture. Figure 7 (NGB, NGB Brief Kickoff, 2003, p. 12) illustrates the private IP network and how National Guard traffic will be secure through the use of a General Routing Encapsulation (GRE) tunnel which will include IP Security encryption. This design provides two large improvements from the current design, as it is physically removed from the

Internet, and within the private network, it is segregated and encrypted. GRE Tunneling allows the National Guard to encapsulate the data packets and encrypt them so that the contents of the packet are not discernable enroute. The only information seen on these packets as they transit the network is the origination point and the destination. These features make the likelihood of any party outside of GuardNet XXI being able to gain unauthorized access to the network extremely small.

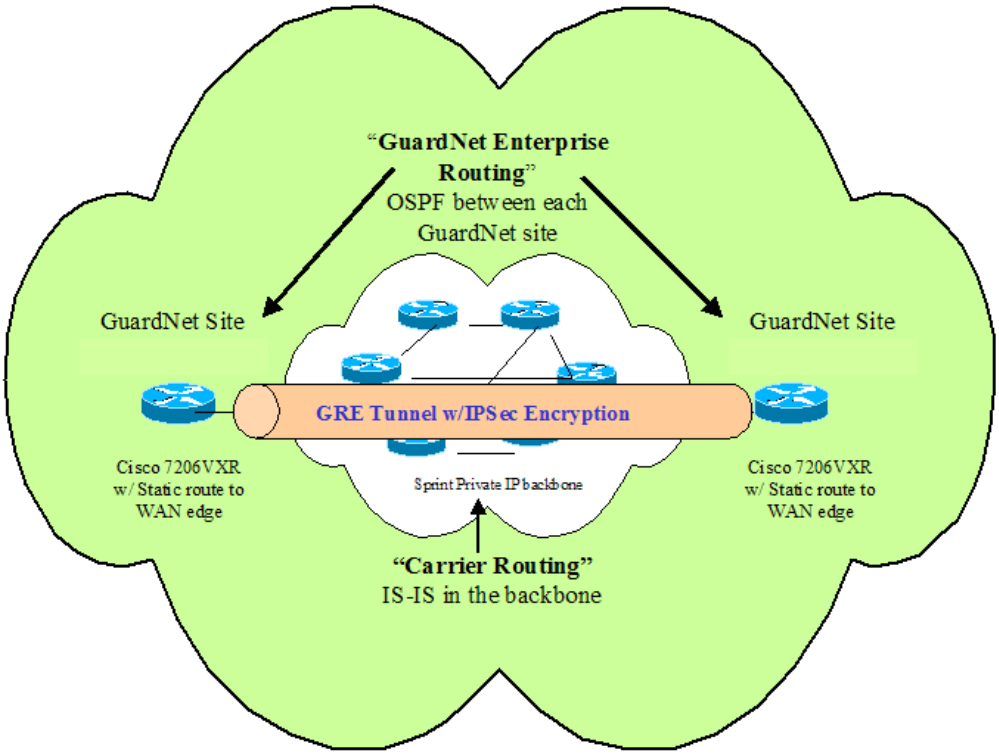

Figure 7. GuardNet XXI Enterprise Routing[7]

[7] OSPF is defined as "Open Shortest Path First" and is a form of dynamic routing

4. The Air National Guard Enterprise Network

Due to the fact that the Air National Guard is funded through the Air Force and has unique requirements separate from the Army National Guard, the Air National Guard maintains its own network separate from GuardNet XXI. The Air Guard Enterprise Network (ANGEN) consists of six regions connected to the Defense Information Systems Network (DISN), which is covered later in this thesis. This regional topology is depicted in Figure 8. (NGB, ANG Enterprise Network Architecture Profile, 2003, p. 5)

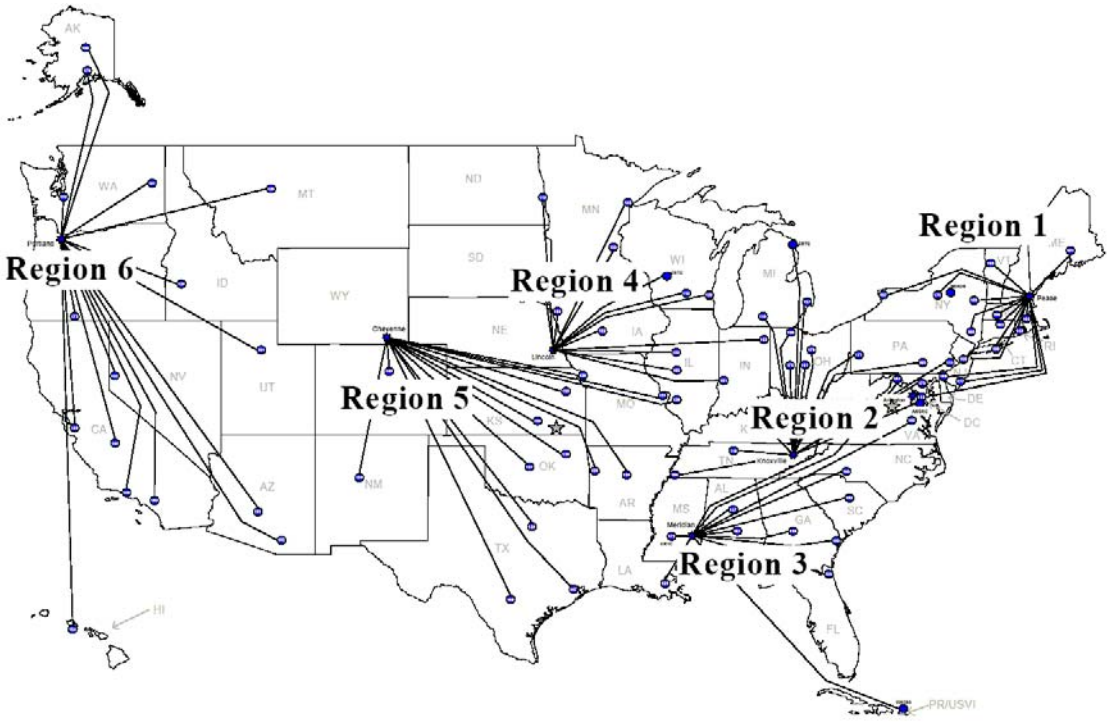

Figure 8. ANGEN regional topology

The ANGEN connects 88 flying wings/bases and 200 geographically separated units to the National Guard Bureau, the Department of the Air Force and the rest of DoD through its connection with DISN. (NGB, ANG Enterprise Network Architecture Profile, 2003, p. 4) At the National Guard Bureau, the Air National Guard maintains a Network Operations and Security Center (NOSC), which operates as the management center for each of the regional nodes containing Regional Operations and Security Centers (ROSC). The ROSCs are connected directly to the DISN and provide T1 connectivity to the 88 flying wings/bases with

an average of 15 wings/bases per ROSC. Each wings and base manages their own LAN to provide services on the facility. This architecture and management platform is depicted in Figure 9. (NGB, ANG Enterprise Network Architecture Profile, 2003, p. 5)

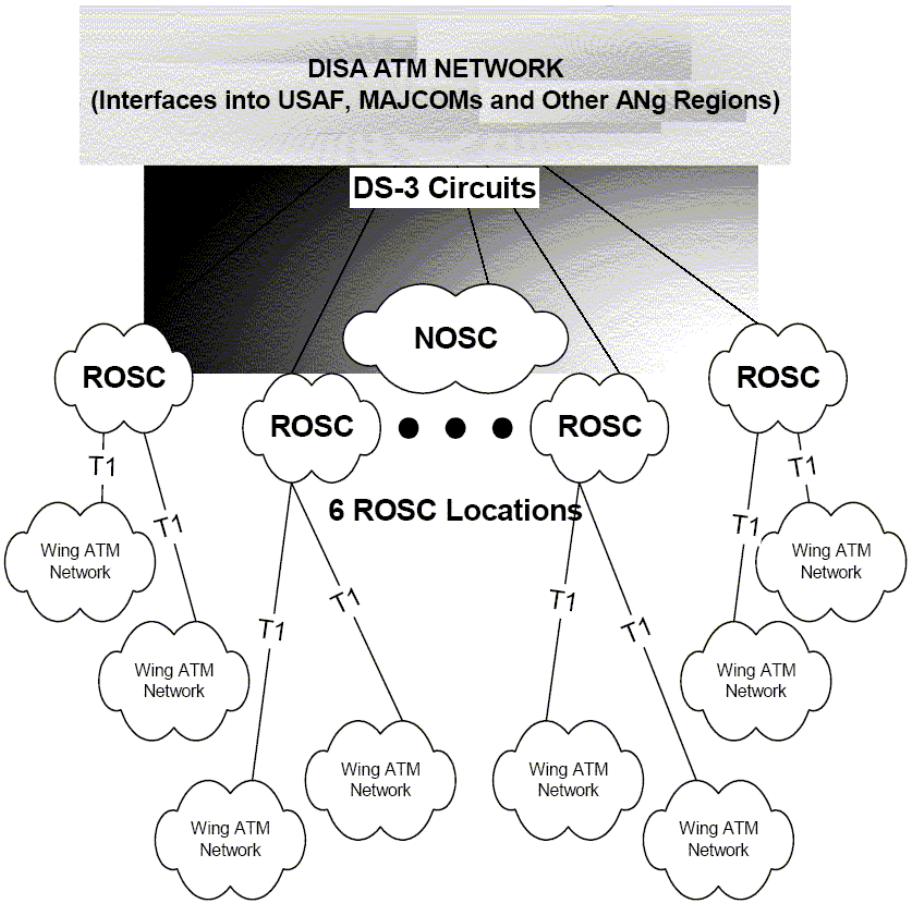

Figure 9. ANGEN Management Platform

5. The Air National Guard Warrior Network

In addition to the terrestrial based GuardNet XXI managed by the Army National Guard and the ANGEN, the Air National Guard maintains a satellite based network called the Warrior Network or WarriorNet. WarriorNet consists of 3 (1.2 mbps – 4 mbps) uplinks to the TelStar 6 satellite which is owned by IntelSat Inc. and over 154 downlinks throughout the United States. The WarriorNet architecture is depicted in Figure 10. (NGB, NGB IT Brief to the United Kingdom ADL Partnership Lab, 2002, p. 30) Through the WarriorNet

downlink and utilizing phone bridging, WarriorNet delivers one way video and two way audio communications.

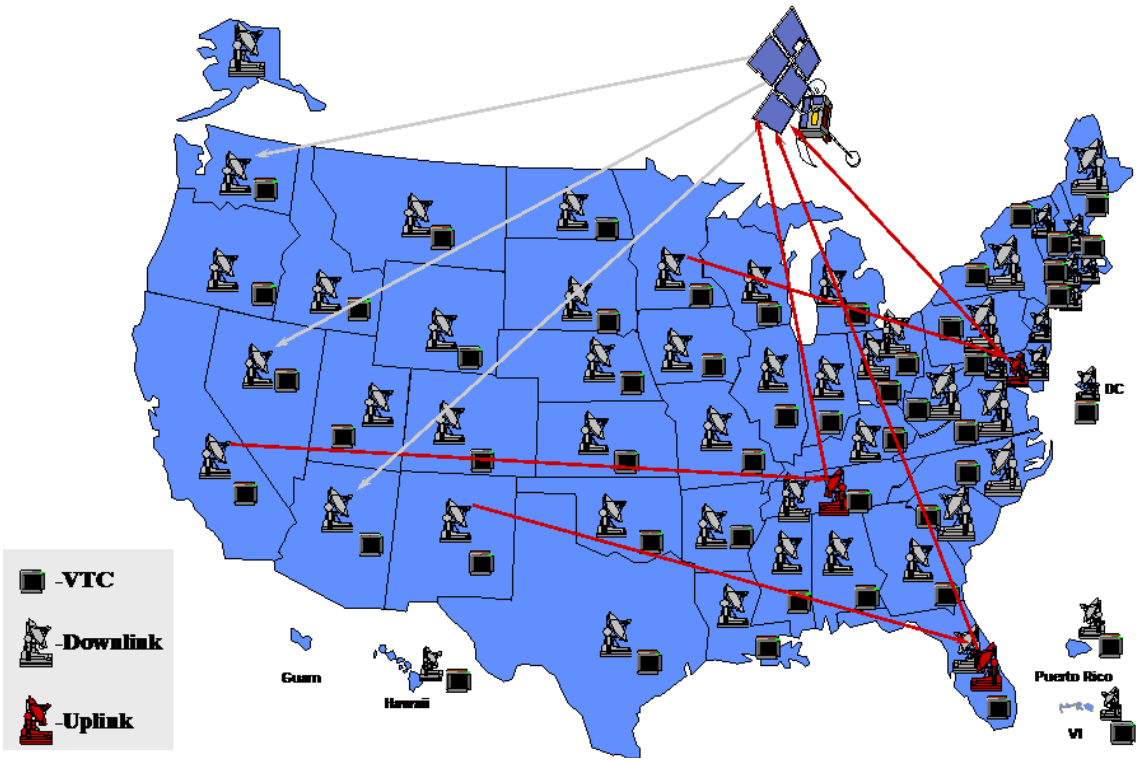

Figure 10. Warrior Network Architecture

Many of the WarriorNet downlinks are co-located with DTTP classrooms and as such, the satellite feed and phone bridging can be pushed through GuardNet XXI as a VTC to all of the 320 DTTP locations. WarriorNet provides an alternative means of communications to the State and local level and provides the National Guard with a back up system should GuardNet XXI fail.

6. The Distributive Training Technology Project

The National Guard Bureau (NGB) is committed to achieving its primary missions of military readiness, rapid response to federal and state needs, and support to peacekeeping operations by leveraging the best instructional methodologies, information systems and communications technologies to deliver education, training, and performance-enhancing tools.

The Army's in-force structure changes have placed a heavy burden on the National Guard to retrain soldiers from one military specialty to another. In the past, such retraining required transporting soldiers to distant classrooms - a costly and time-consuming process. Budget constraints and fiscal responsibility have made it financially unfeasible for the Guard to continue retraining soldiers in this manner.

The Distributive Training Technology Project (DTTP) gives significant opportunity to the Guard to maintain the required readiness, and offset the cost of the program. The advantages of the program to readiness include that it:

- Increases the number of soldiers that can be trained at the same time, lowering the cost of instructors and transportation.
- Reduces the amount of time it takes to deliver requisite training to multiple large groups.
- Broadens the scope of education, making more information available to more people at the same time.

GuardNet XXI currently connects more than 320 multimedia classrooms illustrated in Figure 11, (NGB, Army Knowledge Symposium Brief, 2003, p. 15) ranging in size from two to thirty seats. Current plans call for the installation of 478 classrooms in total by the end of 2006. Communications capabilities include two-way audio and two-way video-teleconferencing, tele-training and Internet access.

DTTP's primary mission is to promote military readiness throughout the Guard and other military organizations by offering access to Advanced Distributed Learning (ADL) tools, technologies, and courseware. Other missions are to enhance command, control, communications, and computers (C4) capabilities; and to make DTTP resources available to other public and private agencies on a cost-reimbursable basis. Because of the network's reliability, DTTP resources have been used to provide communications and other support during times of crisis. Even before 9-11, for example, project personnel were

working to leverage the DTTP system and its network capabilities to support C4 requirements for homeland security. As a result, the DTTP was able to distinguish itself as a crucial and reliable communications tool in the wake of the terrorist strikes on the World Trade Center (WTC). Project personnel established and sustained a critical, continuous 24-hour communications link among National Guard commands in New York, New Jersey, and Connecticut. Command staffs at these sites used the link to coordinate emergency responses, deploy troops, and resolve logistical problems - at a time when land-line and cellular networks were overcome by volume. In Washington, the DTTP also connected National Guard leadership in Virginia, Maryland, and the District of Columbia after the Pentagon attack. Unfortunately, even using DTTP, the State National Guards were not able to integrate all facets of communications.

In addition, the NGB, in partnership with such organizations as the Centers for Disease Control (CDC), the Federal Emergency Management Agency (FEMA), and the National Terrorism Preparedness Institute (NTPI) has been using its terrestrial and satellite networks to support emergency-response training utilizing an existing cooperative agreement framework which allows the shared usage of federal assets by local citizens.

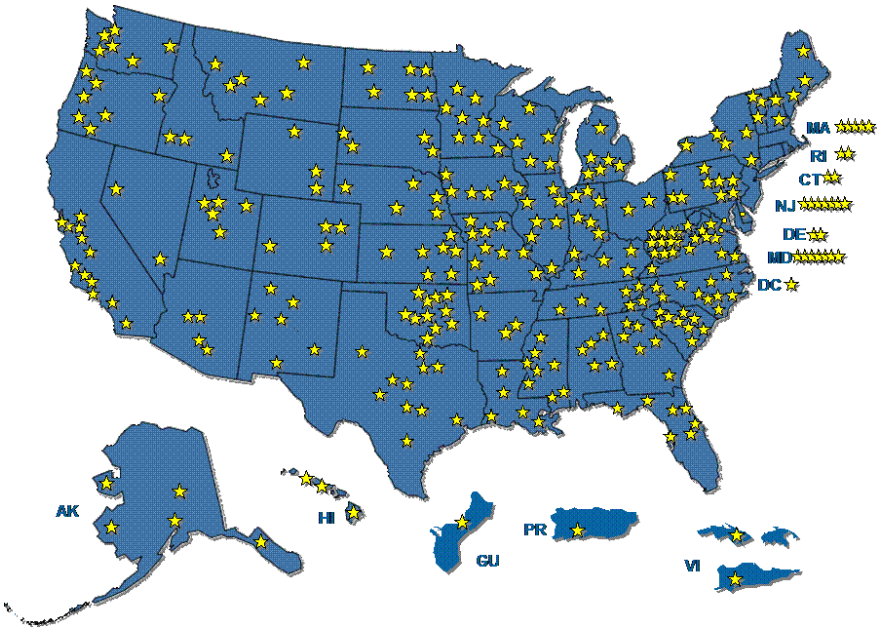

Figure 11. DTTP Classroom locations

Since 9-11, the National Guard has supported more than 20 satellite teleconferences for military and civilian emergency-response communities at more than 500 locations around the country.

A typical DTTP classroom consists of the following equipment and capabilities:

- Tandberg IP video teleconference equipment
- Internet access
- 2 to 33 networked computer workstations (10 average)
- overhead projector
- document camera
- printer and fax machine
- audio conference capability
- WarriorNet downlink (100 classrooms)

7. The Reserve Component Automation System

The Reserve Component Automation System (RCAS), a successful Acquisition Category (ACAT) 1A program, is an automated information management system that serves the Army Guard and the United States Army Reserve forces. The RCAS mission is to,

> …support daily operational, training, and administrative tasks for all Guard and Reserve echelons, and provide timely and more accurate information to plan and support mobilization. RCAS links approximately 10,500 Guard and Reserve units at approximately 4,000 sites located in all 50 states, the District of Columbia, Guam, Puerto Rico, the Virgin Islands, Europe, and the Pacific Rim. (RCAS Website, 2004, p. 1)

RCAS consists of a Commercial off the Shelf (COTS) Personal Computer (PC) based open architecture. According to the RCAS summary brief, RCAS currently

consists of 3857 sites and a total of 57,867 PCs. (NGB, RCAS summary brief, 2002, p. 33) The RCAS system is connected via Guardnet XXI as depicted in Figure 3.

In addition to the hardware fielded through the RCAS program, eight increments of software packages have been fielded from 1996 through 2003. According to the RCAS summary, those software increments provide the following capabilities. (RCAS Website, 2004, p. 1)

- COTS office automation software (Microsoft Inc. Windows based)
- Logistics
- Force Authorization
- Security
- Training
- Human resource management
- Occupational health
- Mobilization planning
- Force Management

Currently, RCAS is in the life cycle support stage of its program, having successfully fielded all eight increments of hardware and software. RCAS provides a point of presence in every state and territory and can be leveraged through GuardNet XXI and the Joint CONUS Communications Support Environment, discussed in the next section, to enhance the flow of information between the incident site and the federal, state and local agencies.

8. The Joint CONUS Communications Support Environment

The Joint CONUS Communications Support Environment (JCCSE), as shown in Figure 12, (NGB, J3 Conference Brief, 2004, p. 5) is a construct that the National Guard Bureau envisions will provide National Guard IT capabilities in support of inter-agency information sharing. The JCCSE will provide

communications across a wide spectrum of networks and platforms at the incident site in support of the National Guard's HLS/HLD mission requirements. Through JCCSE, the incident commander can access information through FM communications, or mobile computing platforms through wireless networks or satellite connectivity. This environment ties together disparate information sources and can provide a common operating picture to the CNGB, US Northern Command (USNORTHCOM) and US Pacific Command (USPACOM) commanders, the Governors and other agency heads. The JCCSE is an umbrella term that provides the National Guard's IT support for the Homeland Security / Homeland Defense environment. JCCSE is not a new network; it is a system of systems, which when aggregated provides the common operational picture.

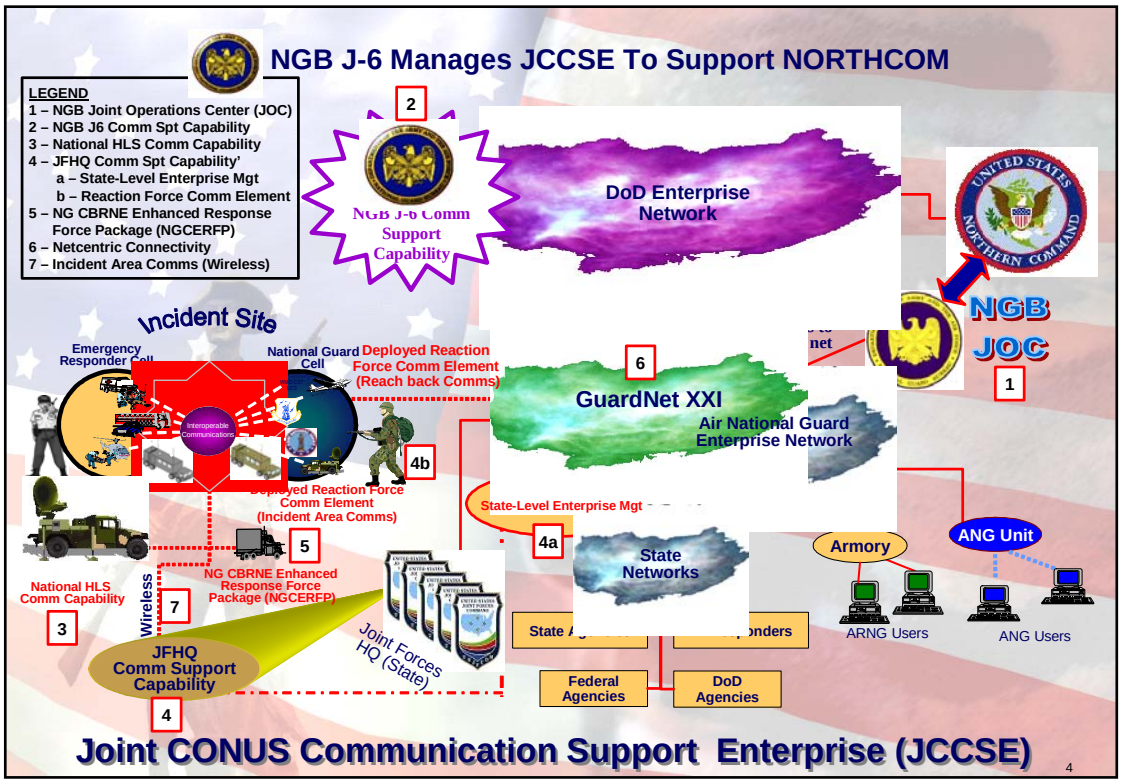

Figure 12. JCCSE

The foundation of the JCCSE consists of a quick reaction force communications element shown in Figure 12, (4b) that is capable of providing interoperable wireless communications and reachback to the Joint Force

Headquarters, State (JFHQ, State) and beyond. The intent of this element is to deploy with National Guard forces in order to provide the required communications support at the incident site. In addition to the quick reaction force and under the umbrella of the JCCSE, the National Guard will field a National Homeland Security Communications Capability. This capability is designed to deploy in support of an incident and provides those basic communications capabilities required under extreme conditions when the local ability to provide them has been destroyed. The National Homeland Security Communications Capability is described in detail in the section on the National Guard's Civil Support Teams. In each of the JFHQ, State, a Joint Operations Center (JOC) will be fielded in order to provide "situational awareness" (NGB, JCCSE Point Paper, 2004, p. 1) so that the Adjutant General of that particular state may have a common operating picture that can be relayed to the JOC at the National Guard Bureau, to Department of Homeland Security (DHS) and to the USNORTHCOM and USPACOM commanders.

As stated earlier, the JCCSE is not envisioned as a new network. JCCSE is envisioned as a construct that ties the existing networks together at the federal, state and local level in order to leverage the unique role of the National Guard in its federal and state missions, providing an integrated picture to the agencies operating within the HLS / HLD environment. This construct simply ties together the existing operations centers and information networks so that information can flow between them securely and seamlessly. LTG Blum explained in his testimony to Congress that the JCCSE

> …will capitalize on existing NGB computer network connectivity throughout the 54 states and territories. If implemented, such a structure could be an important link between the United States Northern Command, the United States Pacific Command, the Office of the Assistant Secretary of Defense for Homeland Defense and other federal and state stake holders. (Blum, 2004, p. 2)

9. The National Guard Bureau Joint Operations Center (JOC)

The National Guard Bureau JOC is where all of the information gathered through GuardNet and WarriorNet is aggregated. It is tied to all 54 JFHQ, State JOCs which mirror the NGB JOC, though not at the same level of capability. Table 1 depicts the capabilities located at the NGB JOC and contrasts them against three JFHQ, State JOCs located in California, Virginia and Maryland. Those capabilities listed in Table 1 (Sullivan, 2004b, p. 1) that have blank squares are not planned capabilities, whereas those that are red are planned but not yet implemented.

		NGB	CA-NG	VA-NG	MD-NG
Voice	Secure Voice (STE/STU)	●	●	●	●
	Non-Secure Voice	●	●	●	●
	Defense Switch Network	●	●	●	●
	Defense Red Switch Network	●			
	Cell Phones	●			
Video	Video Teleconference (VTC	●	●	●	☼
	Secure VTC	●	●	●	☼
	Meridan Integrated Conference Bridge	●	●	●	●
DATA - Systems & Applications	SIPRNET Email & data Exchg	●	●	●	●
	NIPRNET Email & data Exchg	●	●	●	●
	SIPRNET Web Svc	●	●	●	●
	NIPRNET Web Svc	●	●	●	●
	Laptops w/ Modems	●			
	Secure Laptops	●			
	Secure Fax	●	●	●	●
	Non-Secure Fax	●	●	●	●
	Defense Message System	●			
	Global Command & Control System	●	●	●	●
	Military Internet Relay Chat (mIRC)	●			
	Operations & Tracking System	●	☼	☼	☼
Terrestiral	HF Radio Voice/Email	●	●	●	●
	Trunked Radio Sys.	●			
	FM/VHF/UHF	●			
SATCOM	Commercial SATCOM	●			
	UHF Tactical Sattelite	●			
	Secure SATPHONE (Iridium/Immarsat)	●	●	●	●

GREEN	Fully Functional
AMBER	Limited, but Functional
RED	No Capability
Unconfirmed w/Organization	☼

DATE - 040514

Table 1. JOC Capabilities

D. THE STANDING JOINT FORCE HEADQUARTERS, STATE

1. Organization

Recognizing the intent of the Secretary of Defense (SECDEF) that "Joint and combined warfighting is the path to the future" (Blum, 2003, p. 1), LTG Blum directed that all State National Guard's combine the Air and Army National Guard headquarters into a single Standing Joint Force Headquarters, State (Provisional) no later than 1 October 2003 and directed they become fully operational by 1 October 2006. (NGB, JFHQST Transformational Guidance, 2003, p. 2) As of the writing of this thesis, the transformation of the National Guard is ahead of schedule. In his transformational guidance, LTG Blum provided templates for how the JFHQ, State may look. Figure 13 (NGB, Annex D JFHQST Transformational Guidance Organization Charts, 2003, p. 2) shows the template for the organization. Of note, within this organization is the inclusion of the Naval Reserve, the Coast Guard, the Marine Corps Reserve and the Army and Air Force Reserve.

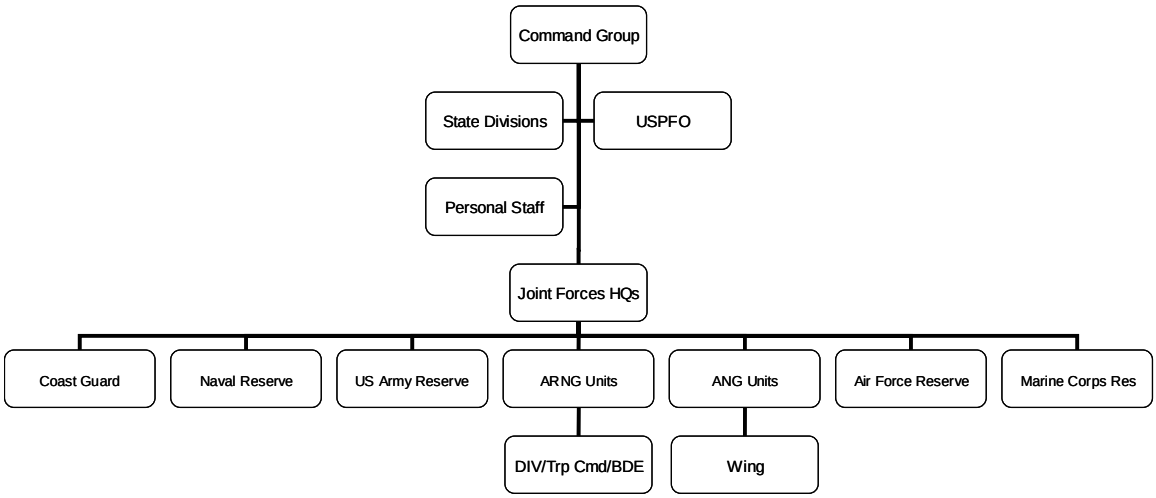

Figure 13. JFHQ, State organizational template

Prior to this change to a Joint Force Headquarters, the Air and Army National Guard had their own Headquarters in the States and the staff did not include the other reserve forces. The intent of creating this new Joint organization was to consolidate

> …162 separate stovepipe Army and Air National Guard headquarters organizations in each state into 54 Joint Force Headquarters – creating a single standing joint force headquarters in each state for all Army and Air National Guard activities. (Blum, 2004, p. 1)

In his testimony to Congress, LTG Blum makes the case that the National Guard and its new Standing JFHQ, State organizational structure is uniquely postured to respond to homeland security and homeland defense incidents at all levels of government.

> In times of emergency, these standing Joint Force Headquarters will provide state Governors with rapid response and better integration of National Guard assistance coming from neighboring states through existing Emergency Management Assistance Compacts. Additionally, these organizations could provide a means for achieving unity of effort by reception and integration of any federal forces which the President might employ in an incident. These headquarters could also, themselves, be federalized. Finally, this headquarters transformation will create efficiencies by consolidating the three separate existing headquarters in each state under one commander, using the manpower saved to fill shortages in lower-echelon units. (Blum, 2004, p. 2)

It is important to note that the National Guard of the Several States, as illustrated in the beginning of this section, is under the command of the State Governor. This fact will weigh on the final organization of each JFHQ, State and it is fully expected that each of the 54 State and Territorial National Guard organizations will look and feel different in accordance with their individual requirements and in accordance with the Governor's intent.

2. Civil Support Teams (CST)

In 1999, Congress funded the creation of the Joint Weapons of Mass Destruction Civil Support Teams. These teams provide support to civilian

authorities in the event there is a chemical, biological or radiological incident, to include disaster, accident or attack. On 9-11, the New York CST was first on scene in Manhattan testing the air to be sure there were no chemical, biological or nuclear materials present. In the Army Field Manual 3-11.22, the Army recognizes the CST as a product of the unique role that the National Guard plays at the incident site. Specifically it states,

> The uniqueness of civil support teams (CSTs) employment and support and the enormity of their tasks must be understood; that is, the concept that results in employment of national guard (NG) CSTs manned by both Army and Air National Guard personnel to support local, state (in Title 32 United States Code [USC] status), and federal (Title 10 USC status) response systems. (FM 3-11.22, 2003, p. 6)

In this section, the Army refers to the dual nature of the National Guard and how the CST specifically can bridge the federal/state gap immediately following an incident. The Governor can, and does, feel very comfortable calling upon the National Guard CST as a first response mechanism, as it is an internal asset to the state. At that point, the CST is a Title 32 force. If and when the incident grows to a level that requires federal assistance, the CST can easily transfer to a Title 10, federal force, or can stay Title 32 and simply become an interface to the federal force. FM 3-11.22 further reinforces this point in saying that,

> As the “governor’s 911 force for weapons of mass destruction (WMD),” the CST provides direct support to the “frontline” of local, state, and federal emergency response organizations. CST operations will primarily occur in a nonmilitary environment that may include urban, rural, industrial, or suburban areas, and/or hot or cold weather environments. Additionally, CSTs will operate only within the US, DC, Puerto Rico, and US territories or possessions while in Title 10 or 32 status. (FM 3-11.22, 2003, p. 6)

In Figure 14, (FM 3-11.22, 2003, p. 10) the DOD consequence management response is illustrated quite well. What this figure shows is the bridge that the CST provides between the federal response and the state response. FM 3-11.22 speaks to the nature of this response and makes the point that,

The line between crisis management and Crisis Management (CM) is blurred. CSTs are state assets whose primary mission supports CM. They may support the crisis management mission (upon request by the appropriate authority) by performing tasks such as collecting an evidentiary sample and maintaining the chain of custody until it is delivered to applicable personnel; but this is secondary to their mission of identifying, assessing, advising, and assisting appropriate authorities at an incident site. They generally perform their mission at the state level. If an event is of the magnitude that the DOD becomes involved, the defense coordinating officer (DCO) may call upon a CST for its CM capabilities. (FM 3-11.22, 2003, p. 9)

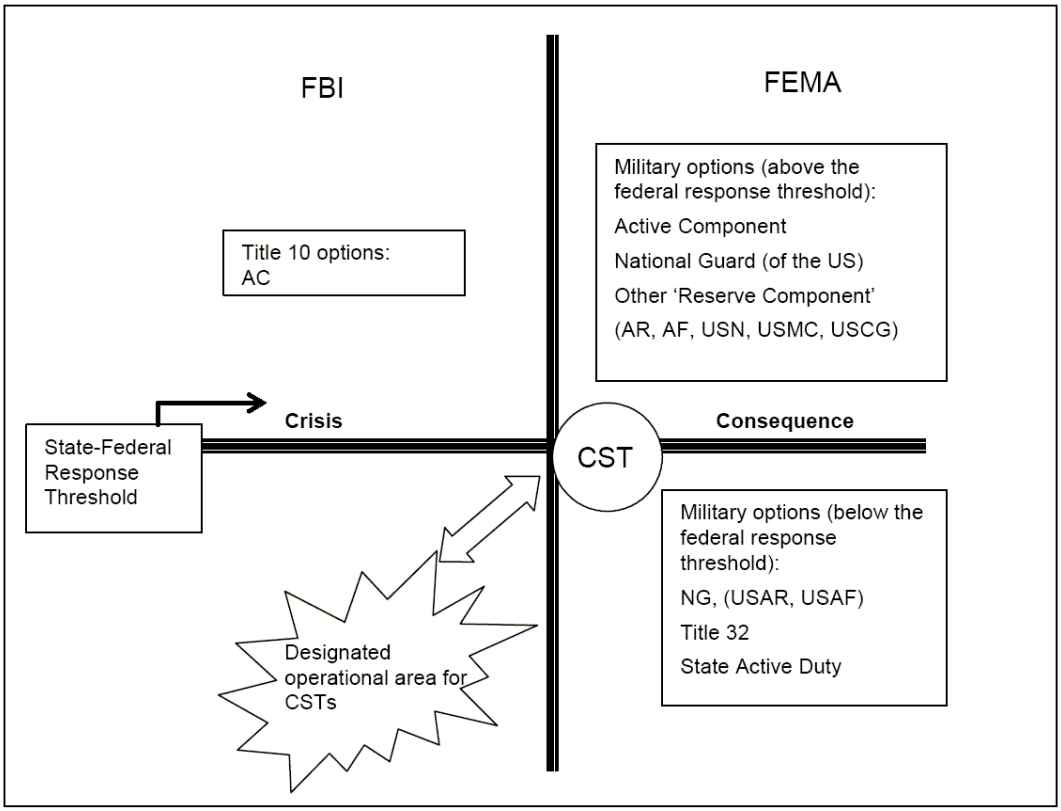

Figure 14. Consequence Management DOD response options

In Figure 14, the horizontal line depicts the border between federal and state and is dependent upon the magnitude of the incident. If the response requires consequence management, at the federal level, FEMA would be the executive agent. Consequence Management is made up of operations that deal with the consequences after an event, usually a natural disaster. If, however, the response requires crisis management, the FBI would be the executive agent.

Crisis Management usually entails a need for law enforcement as it deals with the crisis as it happens. This would occur during a terrorist incident. Below the horizontal line all military support to civil authorities would be in Title 32 or state active duty and above the line would be federal duty, Title 10.

FM 3-11.22 states that the mission for the CST is to,

> …support civil authorities at a domestic chemical, biological, radiological, nuclear, and high-yield explosives (CBRNE) incident site by identifying CBRNE agents/substances, assessing current and projected consequences, advising on response measures, and assisting with appropriate requests for additional support. (FM 3-11.22, 2003, p. 6)

In illustrating how the CST command structure is organized in support of this mission, Figure 15 (FM 3-11.22, 2003, p. 21) again depicts the dual nature of the National Guard. The CST answers directly to the State Governor through The Adjutant General (TAG), yet has liaison and support roles to both the combat commander, USNORTHCOM in CONUS or PACOM in Alaska, Guam and Hawaii, and the incident commander. If required, the CST can be federalized, although it is not necessary as it supports all levels of incident response.

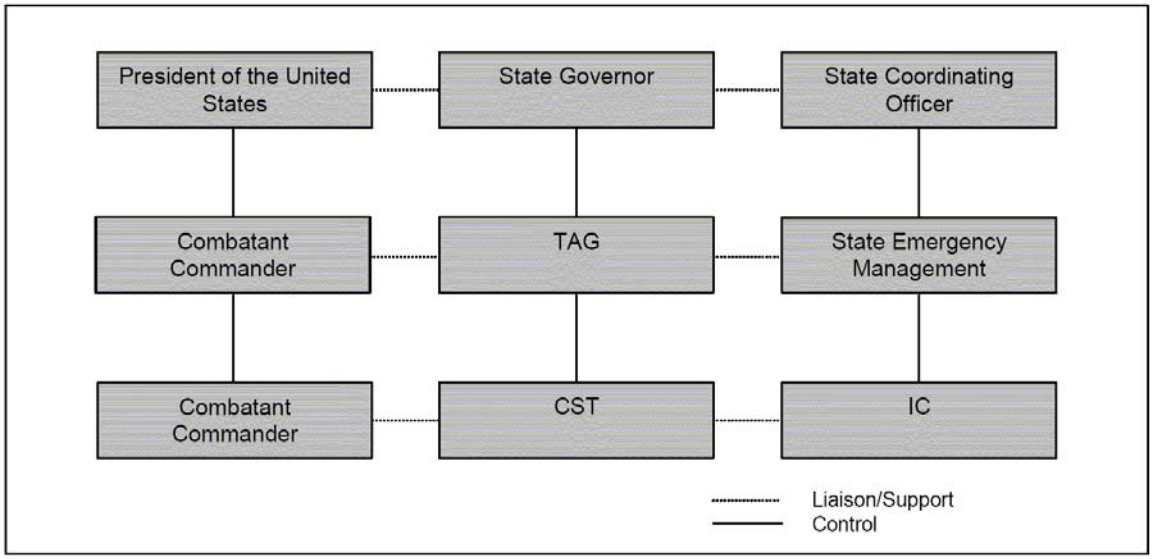

Figure 15. CST Command Structure

Within the CST, the team is organized as illustrated in Figure 16. (FM 3-11.22, 2003, p. 28) The team is made up of 22 members from both the Army

and the Air National Guard. The CST is federally resourced, trained and equipped and it is made up of a multi-disciplinary force that contains a variety of job specialties.

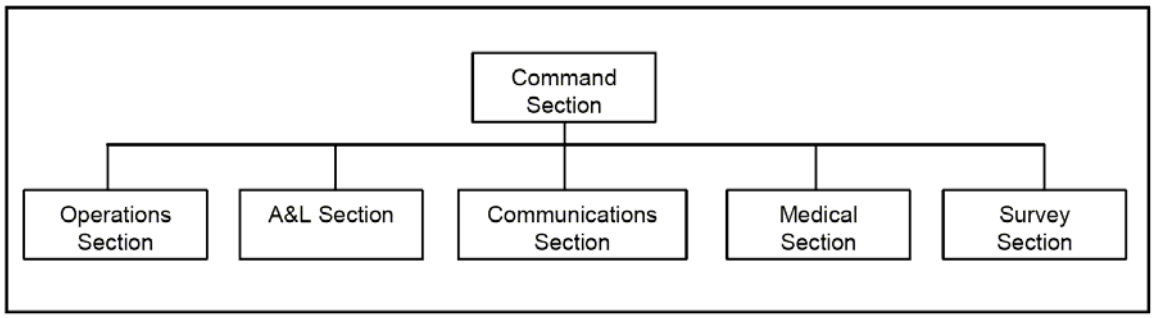

Figure 16. CST organization

As shown in Figure 16, the team is made up of a command section, commanded by a lieutenant colonel, and five sections. Of these five, the communications section is of particular interest to this thesis, as this section is the proposed linkage between the incident commander, their assets in the field and the various agencies at the local, state and federal level.

The communications section consists of two personnel, a communications section chief and an information section officer. FM 3-11.22 states that the task of the communications section is to provide

> …internal and external communications for the unit. The unit interconnects with tactical communications at the incident, transmits situational reports (SITREPs) to the unit's HQ, and reaches back to obtain technical references and advanced modeling. The communications section ensures reliable communications to transmit assessments of the CBRNE situation, provides reach back for information and subject matter expertise, and communicate with higher and supporting HQ. (FM 3-11.22, 2003, p. 32)

In support of its mission, the CST is equipped with eight vehicles. Those vehicles include a Unified Command Suite (UCS), a Mobile Analytical Laboratory System (MALS), and six other command and logistical vehicles. The UCS is the backbone of the CST's communication capability and it is designed to bridge and

communicate across disparate first response and supporting agency frequencies and networks. FM 3-11.22 states that,

> The Unified Command Suite (UCS) provides a technical support interface with robust communications capability across the varied first-responder and support agency frequencies to assist the C2. Through the UCS, the team can perform reach-back activities to other subject matter experts (SMEs) within a number of agencies and connect to key modeling capabilities and labs throughout the US. This reach-back to technical support provides an additional capability for the IC. (FM 3-11.22, 2003, p. 30)

Table 2 (Sullivan, 2004a, p. 1) depicts the capabilities of the UCS as a mobile command post and communications infrastructure that is an essential tool to the incident commander. Supporting the UCS role as an incident response bridge between multiple disparate radio and data networks in support of the Incident Commander, FM 3-11.22 states that:

> The Unit equipment includes… communications equipment, such as the UCS, to provide enhanced architecture and ensure communications and data connectivity between federal, state, and local response forces. The UCS is a self contained, air-transportable system that is capable of continuous fixed and mobile operations. Its capabilities include high-frequency, ultrahigh-frequency (UHF), very-high-frequency (VHF), and tactical frequency-modulated (FM) satellite communications; secure phone; facsimile (FAX) copy; telecomputer; printer; teleconference/video; global positioning system (GPS); and an internal and external power generation. (FM 3-11.22, 2003, p. 34)

Under the direction of the CST commander, the communications section is tasked to provide communications support to the incident. Specifically, the communications mission is to "…provide tactical emergency and garrison communications to the CST commander and as requested by a site IC." (FM 3-11.22, 2003, p. 138) According to doctrine, the communications section provides this support through the UCS which is designed to provide voice and data communications across a wide spectrum of networks designed to support civil and military agencies. The UCS is intended to fulfill the role of "common support node for an incident site." (FM 3-11.22, 2003, p. 138) To fulfill this role, the communications section maintains intra-team communications and

communications with all levels of the incident response as designated by the higher headquarters and the incident commander.

Primary Mission: WMD Incident Response	National Guard, Civil Support Team Unified Command Suite
Capability:	
UHF/VHF/HF Radios	Available
Land Mobile Radios	Available
Ku Band SATCOM	Available
Military UHF SATCOM	Available
INMARSAT	Available
Secure/Non-Secure Voice	Available
Secure/Non-Secure Data	Available
Secure Fax	Available
Secure VTC	Programmed
Wireless LAN	Programmed
DSN/Tactical Telephone	Available
Video feeds	Available
UAV downlink into C2	Under development
GCCS Interface	Available
C-130 Deployable	Available
Military Power Generator (15KW)	Available
Personnel Requirements	2 Personnel

Table 2. UCS Capabilities & Comparison

These communications links extend to other supporting agencies and Subject Matter Experts (SMEs) in order to provide guidance, logistical support and expertise to the incident commander. The communications section also provides classified capable secure communications from the incident site and is completely self contained. The majority of communications from the UCS are high frequency radio and satellite based systems and do not require any local infrastructure at the incident site.

3. State Networks

The National Guard Bureau provides GuardNet XXI to all of the 54 states and territories including the District of Columbia, but this network terminates at the Standing JFHQ, State. From that point to the individual armories, the states, territories and the District are responsible for the design and maintenance of the state portion of the Guard's network. Through the NGB, the federal government assists the states with federal monies, configuration, and security support. As each state National Guard has a unique structure, which is tailored to support the Governor, so too is the state network. Many of the state and territorial National Guard networks connect at the Standing JFHQ, State to additional state and local agency networks.

The State of Iowa is an excellent example of how these networks interface at the Standing JFHQ, State. According to the Iowa Fact sheet, the lower level of the Standing JFHQ, State houses:

- the State Emergency Operations Center (SEOC)
- the Iowa National Guard Emergency Operations Center / JOC
- the Iowa Department of Public Safety Emergency Operations Center and Communications Center
- the Iowa Communications Network central operations center, and
- the Disaster Recovery Backup Computer Center. (Iowa Fact Sheet, 2004, p. 1)

The State of Iowa has designed the Standing JFHQ, State facility to be an alternate site for essential government functions, should anything occur at the state capital complex to compromise its capacity to function. The lower level of the facility meets the Federal Emergency Management Agency's requirement for states to have provisions for continuity of government, (Iowa Fact Sheet, 2004, p. 1) and is hardened with concrete and steel I-beams to provide a 24" barrier to protect from natural or man made disaster. According to the fact sheet, the

JFHQ, State JOC is directly connected “to a system of 2,800 miles of buried cable which represents a highly survivable communications system.” (Iowa Fact Sheet, 2004, p. 1) In addition,

> The Disaster Recovery Computer Center provides a location for the state government's seven major computer centers to conduct operations if one were to become inoperative. The seven major computer centers are located at the three state universities, University Hospitals, General Services, Human Services, and the Department of Transportation. None have the capacity to back up another if one goes down. The backup computer center stores a second copy of all computer tapes on which state government runs, and is configured to provide all necessary connections to connect leased computers in order to bring the computer services back on line. (Iowa Fact Sheet, 2004, p. 1)

The Iowa Standing JFHQ, State is one of the most advanced, interconnected organizations in the country, but all of the states, territories and the District of Columbia have multiple interfaces with disparate networks at the Standing JFHQ, State JOC that can be leveraged to increase the communications footprint that a federal, state or local responder may utilize.

IV. UNITED STATES NORTHERN COMMAND

On 1 October 2002, United States Northern Command (USNORTHCOM) was created by President Bush to serve,

> …as a geographic combatant command to provide "unity of command" for US military actions that counter threats to our homeland from the air, space, land, and sea domains. USNORTHCOM is like any other geographic combatant command, however the United States homeland is included within the area of responsibility (AOR). The total threat picture to the AOR encompasses state symmetric (state on state), state asymmetric (e.g., information warfare), and non-state asymmetric (e.g., terrorism). (United States Northern Command, 2004, p. 15)

Within the United States Department of Defense, the globe is assigned to five combatant commands, USNORTHCOM, United States European Command (USEUCOM), United States Pacific Command (USPACOM), United States Southern Command (USSOCOM) and United States Central Command (USCENTCOM). These assigned areas are called Areas of Responsibility (AORs) and the four surrounding North America are depicted in Figure 17. (United States Northern Command, 2004, p. 30) USNORTHCOM is the Department of Defense's lead agency in the protection of the continental United States territory, domestic population and critical infrastructure against military attacks emanating from outside the country. An attack of this type is considered to be an act of war, and as such, USNORTHCOM's mission is defense of the homeland or "homeland defense". As a military organization, USNORTHCOM's actions within the United States are governed by law under the Posse Comitatus Act, as mentioned earlier. This act prohibits direct military involvement in domestic law enforcement activities and restricts the military's activities to homeland defense and civil support to lead "civilian" federal agencies.

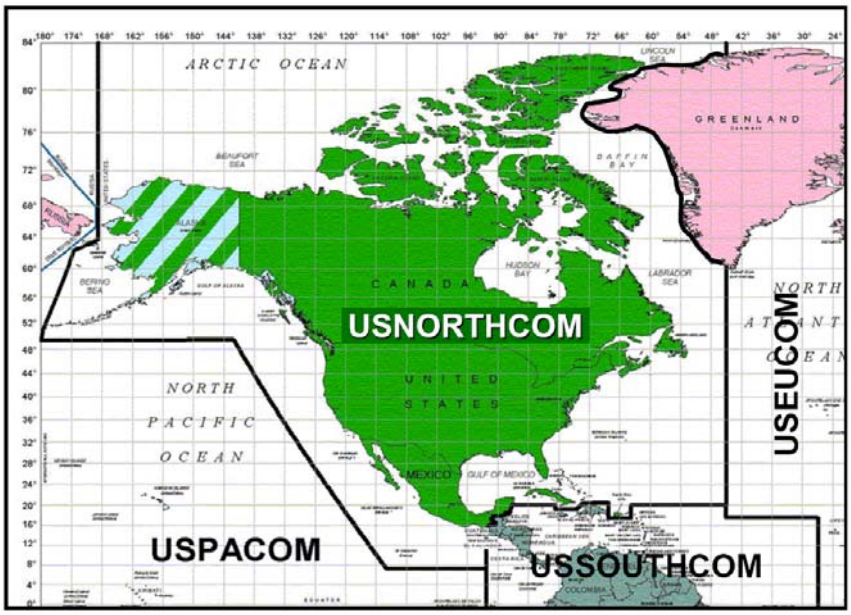

Figure 17. Combatant Commands AORs that adjoin the United States

General Eberhart, the commander of USNORTHCOM, expressed the role of USNORTHCOM well in his testimony to Congress. He said:

> We conduct operations to deter, prevent, and defeat threats and aggression aimed at the United States, its territories, and interests. We also provide military assistance to civil authorities, when directed by the President or the Secretary of Defense (SECDEF). When we work with civil authorities, we will most likely be in a support role to a lead federal agency, providing a single point of contact for federal military assistance. The President's decision to establish USNORTHCOM has enhanced the Department of Defense's (DoD) ability to provide quick, responsive support, when and where needed. (Eberhart, 2003, p. 1)

USNORTHCOM recognizes the uniqueness of the National Guard and how the duality of mission, as discussed earlier, makes the Guard the likely first responder for the military at the incident site. The USNORTHCOM Concept of Operations makes the point that:

> Given the unique operations environment of the AOR, the reserve components, by virtue of their community-based presence, are in a unique position as de facto forward military capabilities throughout the 54 States/Territories. Additionally, the National Guard's [NG] unique dual State-Federal status makes it likely that the National Guard will be employed in State Active Duty [SAD] or Title 32

> [when appropriately authorized] status as soon as the governor[s] determines that a military capability is needed to augment civilian emergency response capabilities. Consequently, in virtually all civil support like situations, the National Guard is likely to be the first military organization engaged at the state-level as well as at the incident area - the "first line of military response." The National Guard can also be leveraged to provide early situational and status information to USNORTHCOM and other Federal stakeholders as the "first line of situational awareness." (United States Northern Command, 2004, p. 28)

A. ORGANIZATION

The Organization chart for USNORTHCOM is depicted in Figure 18. USNORTHCOM's headquarters is located in Colorado Springs, Colorado at the Peterson Air force Base. In order to accomplish its missions, USNORTHCOM utilizes a combination of Joint forces. Joint Task Force – Civil Support, JTF-CS and Joint Task Force – 6, JTF-6 are the two primary task forces that USNORTHCOM relies upon to complete its mission. The USNORTHCOM Concept of operations lays out the roles of both JTF-CS and JTF-6. It states with regards to JTF-CS that,

> JTF-CS plans and integrates DoD support to the designated Lead Federal Agency for CBRNE CM" (consequence management) "operations. When directed by CDRUSNORTHCOM, JTF-CS will deploy to the incident site, establish command and control of designated DoD forces and provide military assistance to civil authorities to save lives, prevent injury and provide temporary critical life support. (United States Northern Command, 2004, p. 42)

With regards to JTF-6, the concept of operations states,

> JTF-6 synchronizes and integrates DoD operational, training, and intelligence support to domestic law enforcement agency counterdrug efforts in the CONUS to reduce the availability of illegal drugs in the United States; and, when directed, provides operational, training, and intelligence support to domestic agency efforts in combating terrorism. (United States Northern Command, 2004, p. 44)

The missions assigned to both JTF-CS and JTF-6 are very closely related to those of the National Guard, and in fact the JTF's and the National Guard

conduct Joint exercises on a regular basis and coordinate their efforts in everyday operations throughout the United States. JTF-CS and JTF-6 are made up of components from the Army, ARNORTH, the Air Force, AFNORTH, the Marine Corps, MARFORNORTH and the Navy, NAVNORTH but are under the operational control of USNORTHCOM. Three interesting relationships are depicted in Figure 18. (United States Northern Command, 2004, p. 39) USNORTHCOM has a coordinating relationship with three force providers that they may draw upon should the need arise. These are NORAD, NGB and the Coast Guard. The USNORTHCOM concept of operations addresses this relationship with NGB; specifically, it states,

> The National Guard Bureau is DoD's official channel of communications on all matters pertaining to the Army National Guard and Air National Guard. As such, USNORTHCOM will foster close and continuous coordination with the NGB and leverage the NGB's capability to facilitate situational awareness, planning, and execution of military support within the States/Territories. (United States Northern Command, 2004, p. 44)

In order to support this relationship, it is essential that there be a continuous presence within the coordinating agencies supporting USNORTHCOM, and that this be supported by IT so that any response to an incident site is a coordinated one.

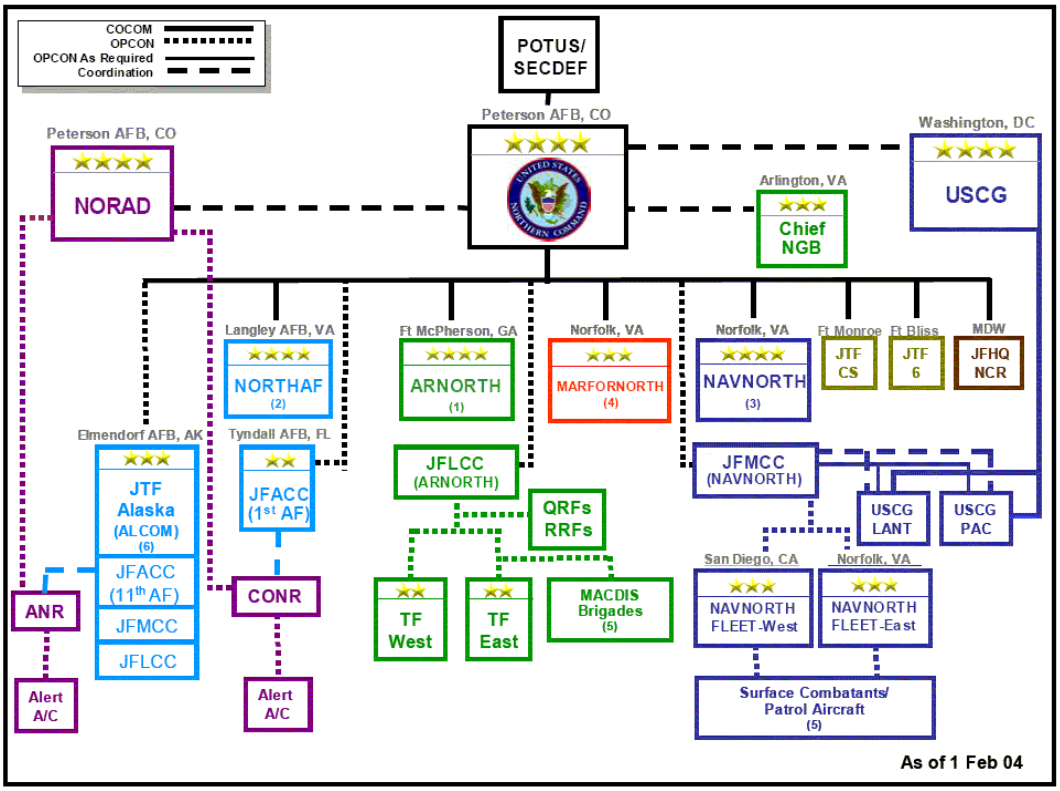

Figure 18. NORTHCOM Organizational Chart

B. MISSION

The mission of USNORTHCOM is stated as,

> USNORTHCOM conducts operations to deter, prevent, and defeat threats and aggression aimed at the United States, its territories, and interests within the assigned AOR. As directed by the President of the United States (POTUS) or Secretary of Defense (SECDEF), USNORTHCOM provides military assistance to civil authorities, including consequence management operations. (United States Northern Command, 2004, p. 27)

USNORTHCOM performs its mission with a graduated response much in the way that the local response is graduated. As the situation becomes more complex and requires greater response, USNORTHCOM can bring more assets to the table. This response is shown in Figure 19. Figure 19 shows that as the event magnitude increases, the response increases. This response begins with providing information at the state level and potential operations such as firefighting and civil disturbance support and gradually increases through

Chemical, Biological, Radiological and Nuclear Events (CBRNE) support to full military intervention in time of invasion or war. It should be noted that the National Guard is the military's first responder and this role is again depicted in Figure 19 (United States Northern Command, 2004, p. 34) under civil support.

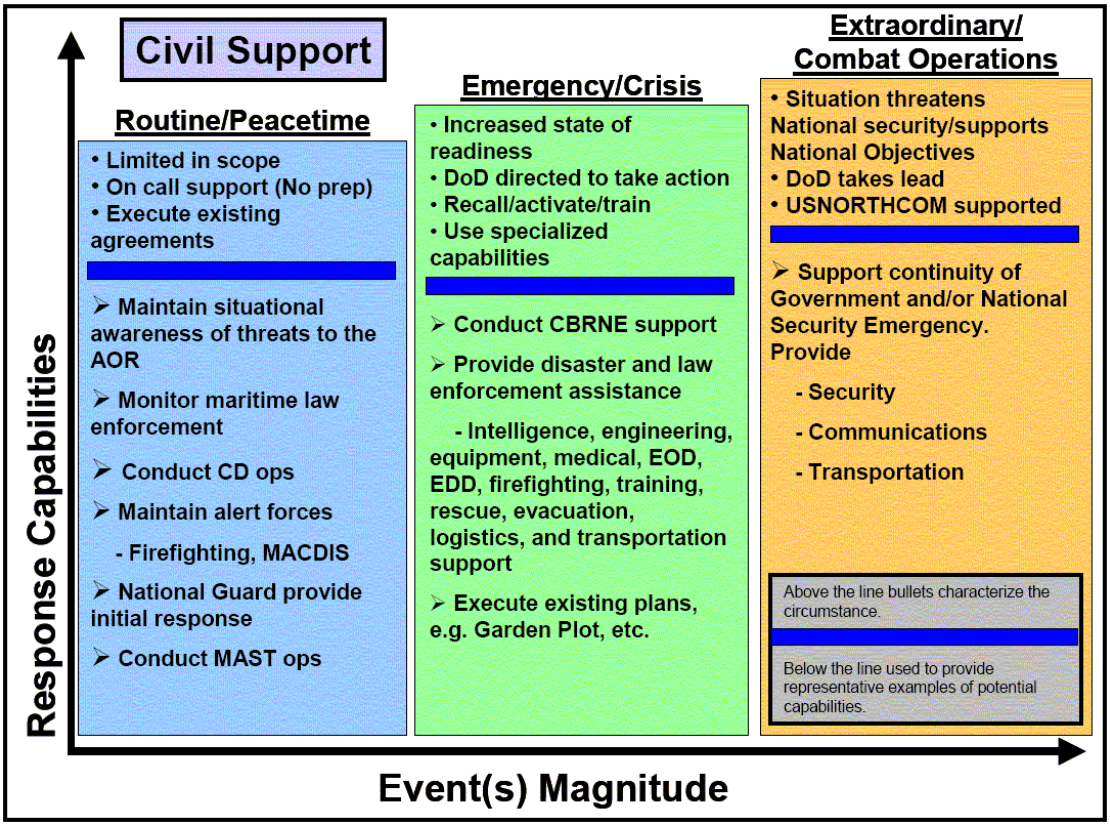

Figure 19. USNORTHCOM Graduated Response

C. THE DEFENSE INFORMATION SYSTEMS NETWORK (DISN)

USNORTHCOM currently utilizes the DISN for connectivity between itself and other DoD entities. DISN is currently made up of secure IP and ATM data communications services, hosts both classified and unclassified networks, and is administered by the Defense Information Systems Agency (DISA).

The unclassified but sensitive IP Router Network (NIPRNet) provides interoperable communications for all combat support activities within USNORTHCOM and it provides access to the Internet. This Internet connection

is also utilized by the National Guard as GuardNet XXI is tied into the NIPRNet. Direct connection data rates on the NIPRNet range from 56Kbps to 155Mbps depending upon the type of connection and the requirements of the organization. (DISN Information Sheet, 2004, p. 1)

The DISN also provides secure classified communications through the Secret IP Router Network (SIPRNet). According to the DISN information sheet SIPRNet is,

> DoD's largest interoperable command and control data network, supporting the Global Command and Control System (GCCS), the Defense Message System (DMS), collaborative planning and numerous other classified warfighter applications. Direct connection data rates range from 56 kbps to 155 Mbps for the NIPRNet, and up to 45 Mbps for the SIPRNet. Remote dial-up services are also available, ranging from 19.2 kbps on SIPRNet to 56 kbps on NIPRNet. (DISN Information Sheet, 2004, p. 1)

Currently, in addition to connectivity to all major installations, SIPRNet is connected directly to all 54 JFHQ, State headquarters for classified information flow. Through connection to DISN, JCCSE can provide the linkage to NORTHCOM directly and to Department of Homeland Security through the NIPRNet Internet ports.

THIS PAGE INTENTIONALLY LEFT BLANK

V. DEPARTMENT OF HOMELAND SECURITY

A. INTRODUCTION

The Department of Homeland Security (DHS) has as its mission to protect the United States against terrorist attacks. To do this, the component agencies within DHS collect and analyze threats and intelligence, guard the borders of the United States and protect its critical infrastructure. In the event of an emergency, DHS has as its role, the coordination of the national response. These missions necessitate that DHS be able to communicate across all levels of government from the federal level to the state and local level including the civilian sector. Additionally, component agencies within DHS have as their responsibility the training for, and implementation of, a coordinated response to a national emergency across all levels of government and the civilian sector. Germane to this thesis are the initiatives that DHS has undertaken in order to bring together the disparate organizations and agencies that it serves to share information and to create a unity of effort for incident response. In its August 2003 report, the GAO noted that:

> Recognizing that information sharing to fight terrorism is a key factor in homeland security, the U.S. Department of Homeland Security has a number of initiatives under way to enhance information-sharing, including the development of a homeland security blueprint, referred to as an enterprise architecture. Through this architecture, DHS plans to integrate the sharing of information within the federal government and between federal agencies, state and city governments, and the private sector. (GAO Report, Homeland Security, Efforts to Improve Information Sharing Need to be Strengthened, 2003, p. 8)

B. ORGANIZATION

The Department of Homeland Security is made up of five major directorates. These directorates, as shown in Figure 20, (Department of Homeland Security, 2004a, p. 1) are:

1. Border and Transportation Security: This directorate is responsible for securing the United States border's and transportation systems.

2. Emergency Preparedness and Response: This directorate is responsible for ensuring that the United States is prepared for and able to recover from both terrorist attacks and natural disasters such as floods, hurricanes and tornadoes.

3. Science and Technology: This directorate is responsible for coordinating the agencies' research and development. A priority of work within the Science and Technology division is research and development of products and systems utilized in response to a weapon of mass destruction.

4. Information Analysis and Infrastructure Protection: This directorate is responsible for intelligence fusion concerning threats to the United States homeland, the issuance of timely warnings to other federal, state and local agencies and preventive or protective action where necessary.

5. Management: This directorate is responsible for managing the budget and personnel within the Department of Homeland Security.

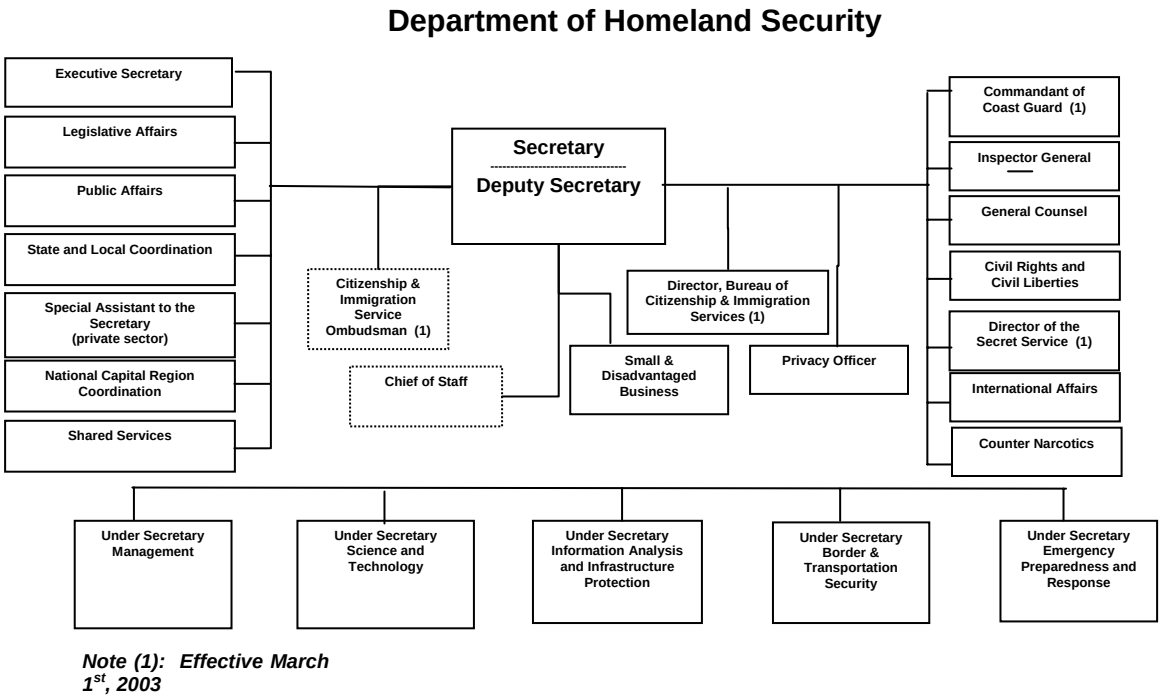

Figure 20. Department of Homeland Security Organizational Chart

In addition to the five main directorates, the Department of Homeland Security also has within it six additional agencies that have either been consolidated under the department or are being created. (Department of Homeland Security Organization, 2004, p. 1)

1. United States Coast Guard: The Commandant of the Coast Guard reports directly to the Secretary of Homeland Security and upon declaration of war, the Coast Guard falls under the command of the Department of Defense.

2. United States Secret Service: The Secret Service has two missions. First, protection of the President and governmental officials and second, protection of U.S. currency from counterfeiting while safeguarding U.S. citizens from credit card fraud.

3. Bureau of Citizenship and Immigration Services: The bureau of Citizenship and Immigrations Services is responsible for providing efficient immigration services and helping to assist incoming immigrants in the transition to American citizenship.

4. Office of State and Local Coordination: The Office of State and Local Coordination is responsible for ensuring close coordination between the federal, state and local responders and their respective governments.

5. Office of Private Sector Liaison: The Office of Private Sector Liaison provides a direct channel of communication between the businesses of the United States and the Department.

6. Office of the Inspector General: The Office of the Inspector General provides DHS with an internal watchdog to safeguard against fraud, abuse and mismanagement.

C. JOINT REGIONAL INFORMATION EXCHANGE SYSTEM

The Joint Information Exchange System (JRIES) is a system that DHS is fielding in an attempt to utilize IT to focus more power on combating terrorism through information sharing and intelligence gathering by thousands of local law enforcement personnel. Currently this system is in its initial phases and as of September 2003, there were 14 states participating in JRIES. JRIES coverage and participation is shown in Figure 21. (Department of Homeland Security, 2003, p. 6)

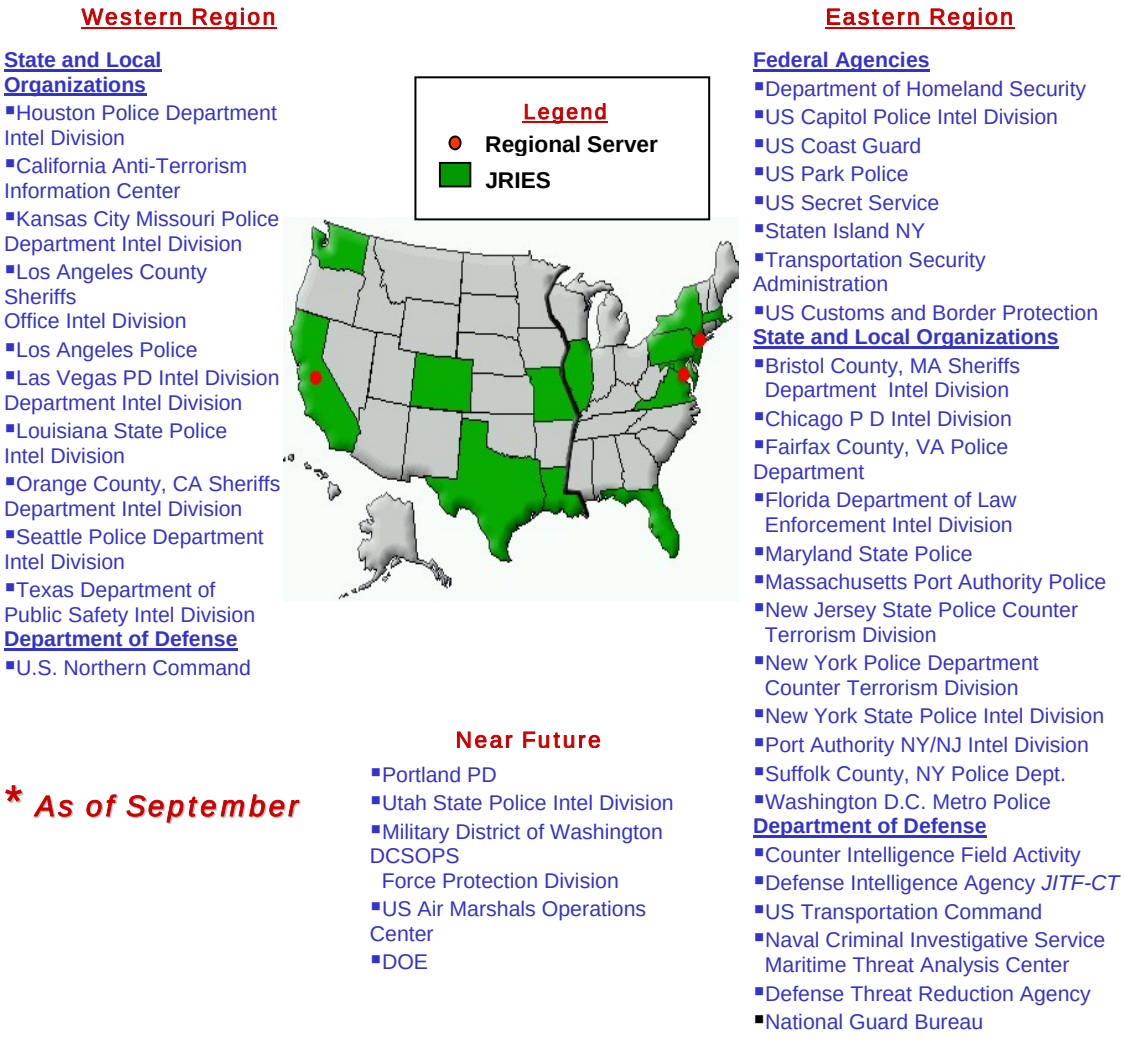

Figure 21. JRIES Participation

According to the DHS JRIES Briefing given to the National Guard, DHS is planning an eventual expansion to all 50 States, and the six Territories and Protectorates. In addition, JRIES will connect to 76 major cities and all 3033 counties across America. According to the brief, specific connectivity planned in those locations includes connections to:

- National Guard: EOC, J-2, Homeland Defense section (connected into JCCSE)
- State Police

- State's Homeland Security Advisors
- State's Emergency Operations Centers

Future enhancements to JRIES will incorporate remaining federal partners and will integrate with other SBU/FOUO (For Official Use Only) networks. (Department of Homeland Security, 2003, p. 7) As of the writing of this thesis, JRIES has been accepted by USNORTHCOM and NGB and has been installed in the USNORTHCOM JOC and the NGB JOC.

Figure 22 (Department of Homeland Security, 2003, p. 13) depicts the DHS integrated architecture that JRIES will reside upon.

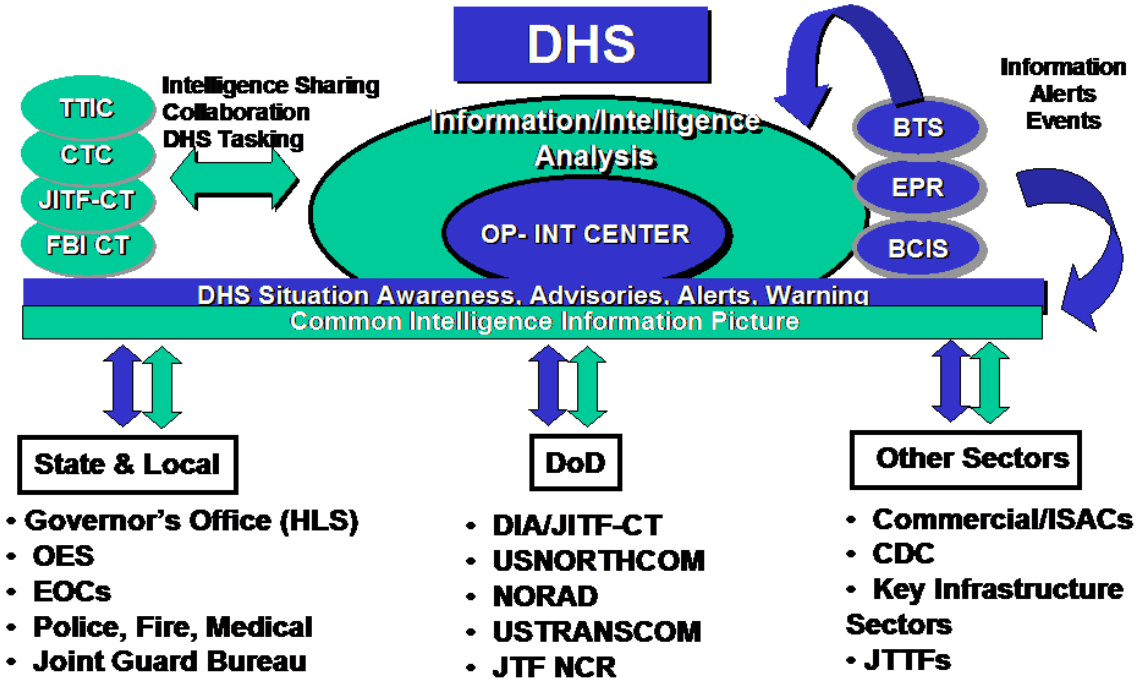

Figure 22. DHS Integrated Architecture

This depiction shows that the DHS operations center is the center of DHS's information/intelligence analysis efforts, but those efforts rely upon a foundation of information and a common operating picture provided to the operations center through interface with many disparate agencies. The National Guard CST team through interface with the NGB JOC and JCCSE can provide that information

linkage to the incident site and assist in aggregating information from the state and local level for transport to the DHS operations center and JRIES.

D. HOMELAND SECURITY INFORMATION NETWORK (HSIN)

In an effort to:

> …strengthen its real time collaborative flow of threat information to state and local communities (HSIN Fact Sheet, 2004, p. 1)

the Information Analysis and Infrastructure Protection Directorate has fielded a commercial off the shelf Internet based counterterrorism collaborative network based upon the Groove Inc. collaborative workspace. HSIN, in its current form, provides secure real time information sharing at the State and local level at the Sensitive but Unclassified Level. The HSIN Fact Sheet states that,

> Future program expansion will include the county level, communication at the classified SECRET level, and the involvement of the private sector. (HSIN Fact Sheet, 2004, p. 1)

The HSIN is designed to interface with the DHS Homeland Security Operations Center (HSOC) utilizing the Joint Regional Information Exchange System, which was discussed in the previous section, and with the NORTHCOM and NGB Joint Operation Centers (JOCs), in order to pass information as required. It is envisioned that through the HSIN, DHS will be able to collaborate real time with each state and major urban area's participants including:

> …governors, mayors, Homeland Security Advisor, state National Guard offices, Emergency Operations Centers, First Responder and Public Safety departments, and other key homeland security partners. (HSIN Fact Sheet, 2004, p. 1)

In order to better understand what HSIN offers, the DHS breaks its functionality into three areas, unique capabilities, collaboration/analysis and information. The HSIN Fact Sheet lists these functions as:

1. Unique Capabilities
    - Communications
    - Low-cost, 24/7 connectivity

- End-to-end encrypted communications

2. Collaboration/Analysis
    - Secure email
    - Interactive collaborative tool (real-time, text or voice)
    - Supports requests for information, exchange, and cross reference
    - Search and Link/Timeline analysis, map/imagery displays
3. Information
    - Daily, periodic, and ongoing report sharing
    - Suspicious incident/pre-incident indicator data
    - Media studies and analysis
    - Mapping and imaging (national, state, county, city)
    - Critical Infrastructure Protection (CIP) information
    - Strategic analysis of terrorist threats, tactics and weapons

(HSIN Fact Sheet, 2004, p. 1)

E. SAFECOM

The Wireless Public SAFEty Interoperable COMmunications (SAFECOM) program, under the Department of Homeland Security, is exploring solutions and standards for the public safety interoperable communications within the incident area, and is an umbrella program that encompasses various public safety wireless initiatives and involves wide-ranging activities. SAFECOM has as its goal, to ensure that all first responders can communicate with each other. Recognizing that it will be many years before they will all have compatible devices, SAFECOM in the short term, is focusing on hardware that will allow disparate communication devices to interface with each other. In a DHS response to the April 2004 GAO report on SAFECOM, DHS explains:

> The SAFECOM program works with existing federal communication initiatives and key public safety stakeholders to coordinate the development of better technologies and create processes to support the cross-jurisdictional and cross-disciplinary coordination of existing systems and future networks. SAFECOM was established as the umbrella program within the federal government to help local, tribal, state and federal public safety agencies improve public safety response through more effective and efficient interoperable wireless communications, which SAFECOM defines as the ability of public safety agencies to talk across disciplines and jurisdictions via radio communications systems, exchanging voice and/or data with one another on demand, in real time, when needed and authorized. (GAO Report, Project SAFECOM, 2004, p. 18)

SAFECOM was initially started under the Office of Management and Budget (OMB) e-government initiative with the managing partner for the program being the Department of Treasury. In May of 2002, the Federal Emergency Management Agency (FEMA) was assigned the role of managing partner and the managing partner was again changed in May of 2003 as DHS took up the role. (GAO Report, Project SAFECOM, 2004, p. 11) According to the April 2004 GAO report:

> This lack of sustained, committed executive leadership hampered SAFECOM's ability to produce results tied to its overall objective. (GAO Report, Project SAFECOM, 2004, p. 11)

Since taking on the role as managing partner in May of 2003, DHS has committed to the SAFECOM program. Though SAFECOM has been slow to evolve, the need to bridge disparate networks has not slackened and DHS has expressed that it will continue to pursue this program. The April 2004 GAO Report recommended that:

> …the Secretary of Homeland Security direct the Under Secretary for Science and Technology to complete written agreements with the project's identified stakeholders, including federal agencies and organizations representing state and local governments. These agreements should define the responsibilities and resource commitments that each of those organizations will assume and include specific provisions that measure program performance. (GAO Report, Project SAFECOM, 2004, p. 16)

The National Guard Bureau J6 is a committed federal partner with the SAFECOM program and is an active participant. Currently, the National Guard is participates in the Rapid Emergency-level Interim Communications Interoperability (RELICI) project (now referred to as “Rapid Comm 9/30”), is a participant on the SAFECOM advisory committee and actively participates in the Federal Partnership for Interoperable Communications (FPIC), a sub committee of SAFECOM for federal entities.

F. PRE-POSITIONED EQUIPMENT PACKAGES

Through a cooperative effort with the Department of Justice, Department of State, Office of Domestic Support, U.S. Department of Justice (ODS) and the Marine Corps Command, the Department of Homeland Security, Office of Domestic Preparedness (ODP) has established 11 Pre-positioned Equipment Packages (PEP). PEP will contain identical equipment so as to standardize maintenance and training. These packages are intended to replenish up to 150 fire fighters, law enforcement, medical teams and urban search and rescue organizations. According to a DHS briefing on PEP, the mission of the PEP program is to:

> Procure, kit, ship, store, maintain, deploy, and replenish Ten or more Pre-positioned Equipment Packages Configured to reconstitute emergency response Organizations during the 12-24 hour period following a Terrorist attack using Nuclear, Biological, Chemical, Radiological, or Conventional High Yield Explosive Weapons of Mass Destruction. (Office of Domestic Preparedness, 2004a, p. 3)

According to the briefing presented in April of 2004 (Office of Domestic Preparedness, 2004a, p. 4), these packages consist of:

- Chemical, Biological, and Radiological Detectors
- Personal Protective Equipment
- Decontamination Equipment
- Communications Equipment

- Bunker Gear
- Urban Search and Rescue - Technical Search Equipment
- Medical Equipment, prophylaxis, and medications
- Transportation, packaging, and material handling equipment

Notably in the PEP, ODP has included a number of pieces of communications equipment. It is recognized by the PEP working group that,

> Experience at prior major incident sites revealed serious obstacles to inter agency communications; thus the PEP Working Group deemed interoperable communications crucial. A complete field mobile communications system will be transported to the scene to enhance the availability of first responders to have interoperable radio and data communications at the scene. (Office of Domestic Preparedness, 2004b, p. 1)

An in depth look at the PEP communications equipment list major end items results in the following: (Office of Domestic Preparedness, 2004b, p. 2):

- Individual communications components:
  - 50 Level A in-suit communication links
  - 4 sets of 50 field programmable portable radios in separate spectrum: 148-174 MHz; 403-457 MHz; 450-512 MHz; and 800 MHz including battery packs, and Yagi and co-linear antennas that span portions of their respective frequency spreads
  - Sixty speaker microphones
- Four laptop computers—two for logistics and two for programming
- Two satellite phones
- 4 cellular telephones

- 5000-watt generator and an uninterruptible power supply

For execution of the PEP project, ODS is the executive agent and develops the protocols for deployment of the PEP equipment. Marine Corps Systems Command (MARFORSYSCOM) manages the acquisition of the equipment and is funded through the ODS equipment grants. MARFORSYSCOM is additionally responsible for outsourcing all maintenance and training for the PEP and is tasked with replenishment as required. ODP is responsible to alert MARFORSYSCOM in the case of expected or imminent incident and to deploy the equipment should a need arise. In addition, ODP provides accountability for equipment on site and is responsible for loaning equipment to other agencies if required. Two issues that have yet to be resolved are who operates the equipment once it is deployed, since local first responders are not trained to operate it, and who coordinates the required airlift in order to move the PEP equipment so that the allocation is made before a terrorist event.

The PEP when deployed must be accessible at the incident site in a timely manner and must sustain the first response community for up to 24 hours. This has led to the requirement that all PEP must be located within one hour of a commercial or military airfield and must have easy access to major thoroughfares and rail. The geographic location of the PEP equipment is depicted in Figure 23. (Department of Homeland Security, 2004b, p. 1)

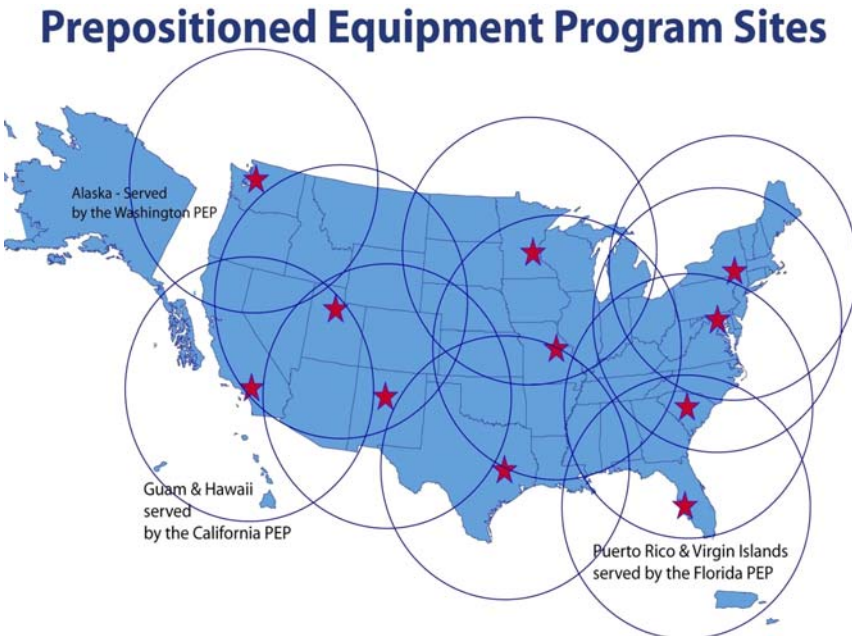

Figure 23. PEP Locations

Each of the PEP sites will be pre-packaged in pods that are transportable and accessible. The PEP is an essential piece of the puzzle that will have to assist in bridging the incident response digital divide as it will become a portion of the communications infrastructure that responds to a major terrorist incident. It is critical that this system interoperate with existing systems, the National Guard UCS and the JCCSE in order to compliment existing infrastructure and seamlessly blend with existing networks.

THIS PAGE INTENTIONALLY LEFT BLANK

VI. PILOT AND DEMONSTRATION PROJECT CASE STUDIES

In this section, I will describe four pilot and demonstration projects in order to show the type of efforts underway across the United States in support of bridging the incident response digital divide. This section is not intended to be an exhaustive listing as there have been dozens of initiatives funded that attempt to solve one or more pieces of the puzzle that makes up this problem.

A. NATIONAL EMERGENCY AND DISASTER INFORMATION SYSTEM (NEDIS)

The NEDIS pilot project is intended to interface with the NGB JCCSE infrastructure in order to provide a database of information that will be available to the first responder at the incident site. The NGB J3 NEDIS briefing states that:

> National Emergency and Disaster Information System (NEDIS) is a World Wide Web accessible database of organizations, skills and expertise, emergency equipment, best practices, lessons learned, and mapping data. NEDIS provides a capability for the collection, analysis and dissemination of information and expertise critical to the coordination of responses as the first military responder to a terrorist attack upon domestic soil. (NGB, NGB J3 NEDIS Brief, 2004, p. 16)

NEDIS was funded through a congressional action and is envisioned to be fielded in three major phases. Those phases are:

1. Proof of Concept (Completed in 2002)
2. System Development and initial implementation (Current)
3. Full implementation

Figure 24 (NGB, NGB J3 NEDIS Brief, 2004, p. 13) shows the interface that is envisioned between NEDIS and JCCSE as NEDIS becomes an information source input into JCCSE.

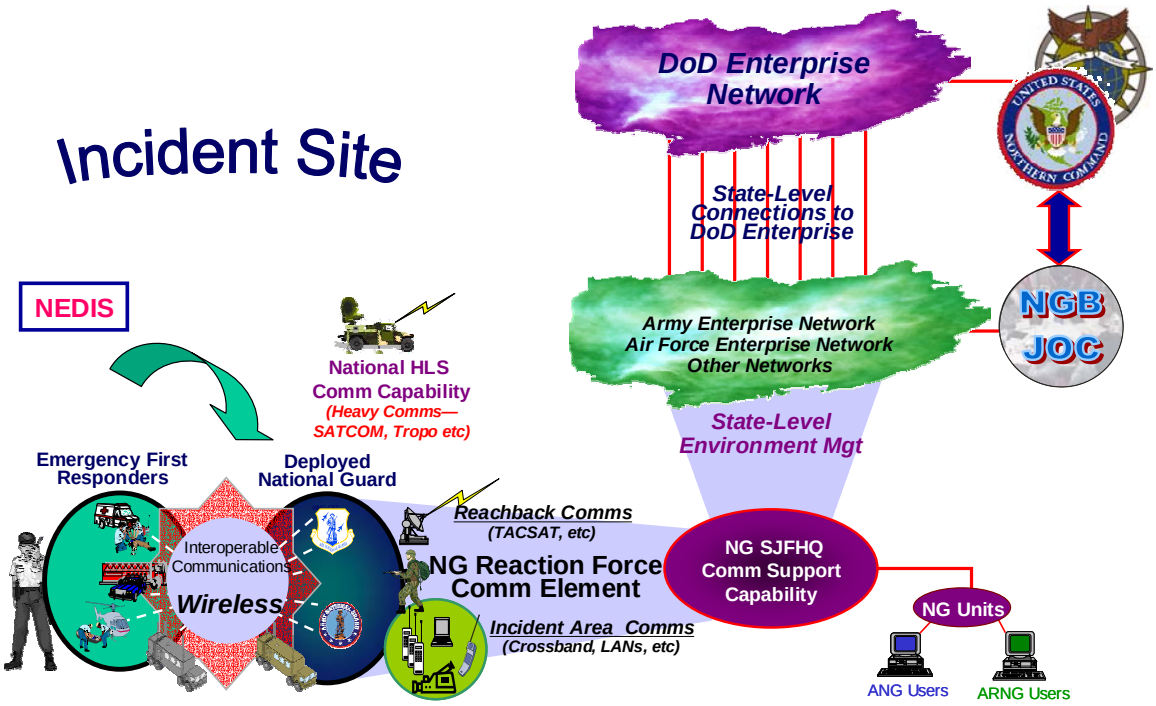

Figure 24. NEDIS Relationship to JCCSE

NEDIS is considered an Incident "Diagnosis and Treatment" System. It will consist of two levels, the enterprise level and the incident level. In terms of hardware, NEDIS will be made up of a data repository and a number of hand held devices. The NEDIS Concept of Operations calls for six progressive and building scenarios that will add capability and complexity to the system. The first scenario is a "routine incident where no additional resources are required." (NGB, NGB J3 NEDIS Brief, 2004, p. 8) In this scenario, there will be a single NEDIS device and it will not need to interface or communicate outside of the incident site. It is anticipated that this scenario covers up to 80% of incidents that first responders will encounter. In the second scenario there is a "routine incident where communications are available." (NGB, NGB J3 NEDIS Brief, 2004, p. 8) In this scenario, there will be added communications back to the 911 center and the EOC. In scenario three there will be an "incident where multiple NEDIS devices are available." (NGB, NGB J3 NEDIS Brief, 2004, p. 8) In this scenario, the NEDIS database will break the single incident checklist that the first responders utilize into sub checklists and will add the enhanced capability for

intra-site communications. In scenario four, there will be an "incident where additional resources/support are required." (NGB, NGB J3 NEDIS Brief, 2004, p. 8) This scenario is anticipated to account for the other 20% of incidents that first responders encounter and will require interaction with the EOC to coordinate the requests for additional support and resources. Scenario five will be an "incident where outside input is required – e.g. Subject Matter Expert input." (NGB, NGB J3 NEDIS Brief, 2004, p. 8) This scenario will require the external experts to input data into the NEDIS database and this data must be searchable and available at the incident site to the first responders. In the final and sixth scenario, there will be "an incident where outside access is requested/required." (NGB, NGB J3 NEDIS Brief, 2004, p. 8) In this scenario, external entities will receive output from the NEDIS database in order to enhance situational awareness and assist in formulating a common operating picture. It is envisioned that at this point, NEDIS will interface with JCCSE in order to receive data from experts and to push data into the Standing JFHQ, State JOC and the NGB JOC. This data would then be available to USNORTHCOM, USPACOM and DHS.

B. EXTENDED RANGE WIRELESS LOCAL AREA NETWORK (WLAN)

The typical extended range WLAN consists of a transmitting entity and multiple wireless access points. With today's technology, many of us have access to the Internet via wireless either through 802.11b or 802.11g, but these are relatively short range and are line of sight. Northrop Grumman Inc. has designed one solution to extending the reach of the WLAN to the incident site. With their design, they extend the Wide Area Network (WAN) that is terminated at a public building by providing connectivity to the fiber that terminates in that facility to a wireless access point. The responding vehicles would be equipped with an extended range, amplified wireless system that would allow connectivity between the mobile computing platform and the access point located strategically at one of the public buildings or at a cell tower. Figure 25 (Northrop Grumman, 2004, p. 6) depicts WLAN connectivity to the response site.

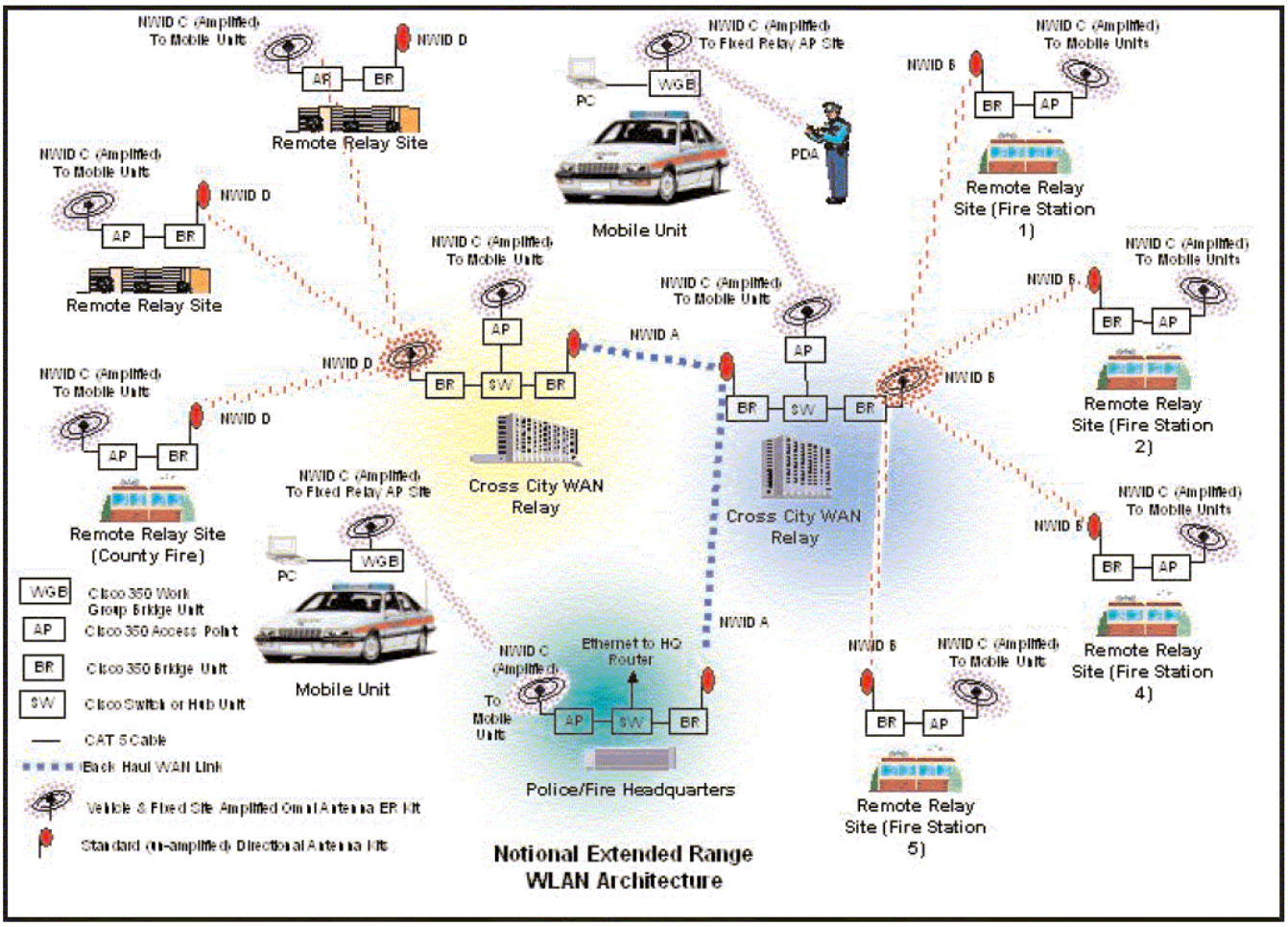

Figure 25. Extended WLAN

According to Northrop Grumman's white paper:

> The main purpose for this high-speed mobile WLAN is to allow for the transfer of administrative non-urgent data traffic and other types of large data file transfers (such as records management files, photos or video, field reports, surface map updates, crime reports, etc.) to be rapidly transmitted and/or received between the vehicle MDC and the agency headquarters (i.e., police, fire, or other County agency). This frees the agency's currently employed data communication system to focus solely on supporting the more critical (low data rate) data and/or voice communications such as dispatch and AVL communications. (Northrop Grumman, 2004, p. 5)

As depicted in Figure 25, this system would allow the first responder to access information at the incident on a Personal Data Assistant (PDA) via wireless

802.11b through the mobile access point, their vehicle or command vehicle, which is tied to the main WAN and their agency's LAN through an extended range WLAN and fiber. This would allow for information flow from the EOC to the incident and back. This type of system is one of the enablers that would allow for a common operating picture to flow between the incident, the EOC, the standing JFHQ State JOC, NGB JOC, USNORTHCOM, USPACOM and DHS.

C. EMERGENCY RESPONSE SYSTEM INTERFACE NOTIFIER

The Emergency Response System Interface Notifier is a Windows Desktop system that was constructed utilizing GIS satellite mapping images and Commercial-Off-The-Shelf (COTS) software from Microsoft Inc. This system was constructed for the county of Fairfax, Virginia in order to demonstrate the value and ease of importing GIS data into an application in support of first responders. When designed, Notifier was demonstrated for the Fairfax-Falls Church Community Service Board (CSB). The CSB is responsible for:

> …the provision of quality mental health, mental retardation, alcohol and drug, and early intervention services to more than 20,000 people a year. Services are provided in more than 16 outpatient clinics and 350 residential sites throughout Fairfax County and the Cities of Fairfax and Falls Church, Virginia. (Dennis, 2004, p. 1)

Federal Law and State laws mandate how the CSB must interact with the first responder community in order to evacuate its special needs patients in the event of natural disaster or terrorist attack. The Notifier system utilizes a secure connection to the CSB database in order to plot the physical location of those patients within the county. Utilizing this data and a plot of the incident area, CSB is given a picture of who needs evacuation and their location, as depicted in Figure 26. (Dennis, 2004, p. 2)

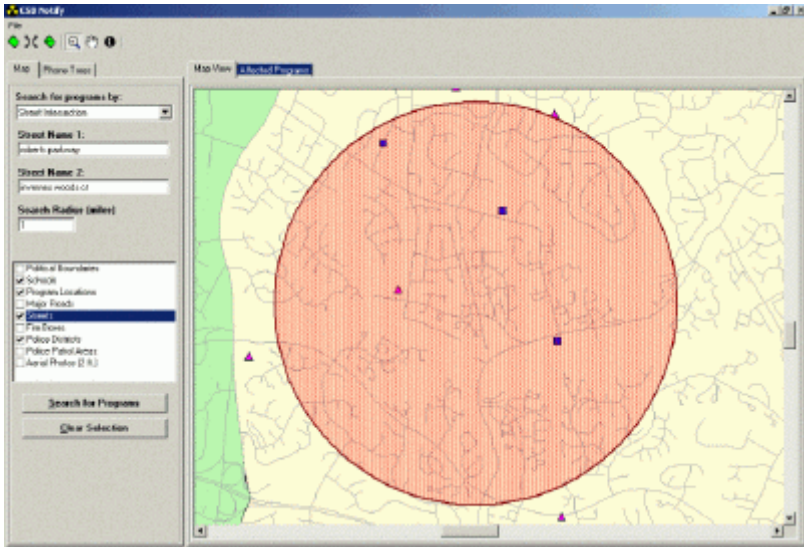

Figure 26. An incident plot with patient's locations

In addition to depicting those needing care, Notifier has embedded in it a phone tree system that will allow for the CSB to easily contact the first responders of those needing special care and of their location. This system allows for zooming into the area and high resolution photographic images to be displayed for a better picture of the situation for the responder. This system is designed to be run from a laptop at either the incident site or, more likely, as a station at the state or county EOC. ESRI Notifier is an example of the type of information that is gathered that can be utilized to create situational awareness. This system is one of many that would require integration into the common operating picture that is fused at the EOC and ported through JCCSE.

D. AUTOMATED EXERCISE AND ASSESSMENT SYSTEM (AEAS)

The AEAS is a system designed and fielded by the National Guard that is designed to exercise and assess emergency response procedures at the jurisdictional level from the local municipality up to the State. According to the AEAS fact sheet:

> AEAS supports common terminology, standardized ascendancy, integrated communications, unified command structure, consolidated action plans, designated incident facilities (command post, staging area, etc.), manageable span-of-control, and com-

> prehensive resource management based on the Incident Command System (ICS) and supplemented by mutual aid compacts and protocols that accommodate regional and state-level participation. (NGB, AEAS Fact Sheet, 2003, p. 1)

AEAS, as designed and fielded by the National Guard Bureau, is available free of charge to local emergency response communities as a tool to exercise their response to a WMD incident. It is designed to allow emergency response agencies to exercise their response to an incident in a simulated environment and discover strengths, weaknesses and interoperability shortfalls such as radio frequencies, manpower issues, communications procedures, etc. In its current form, AEAS simply exercises emergency response agencies within a state and how those agencies interact with some of the federal agencies, but by utilizing this system, the potential exists to connect this simulation through JCCSE to the standing JFHQ, State JOC, the NGB JOC, the USNORTHCOM and USPACOM JOC and DHS HSOC in order to prove connectivity and to exercise the national response to an incident.

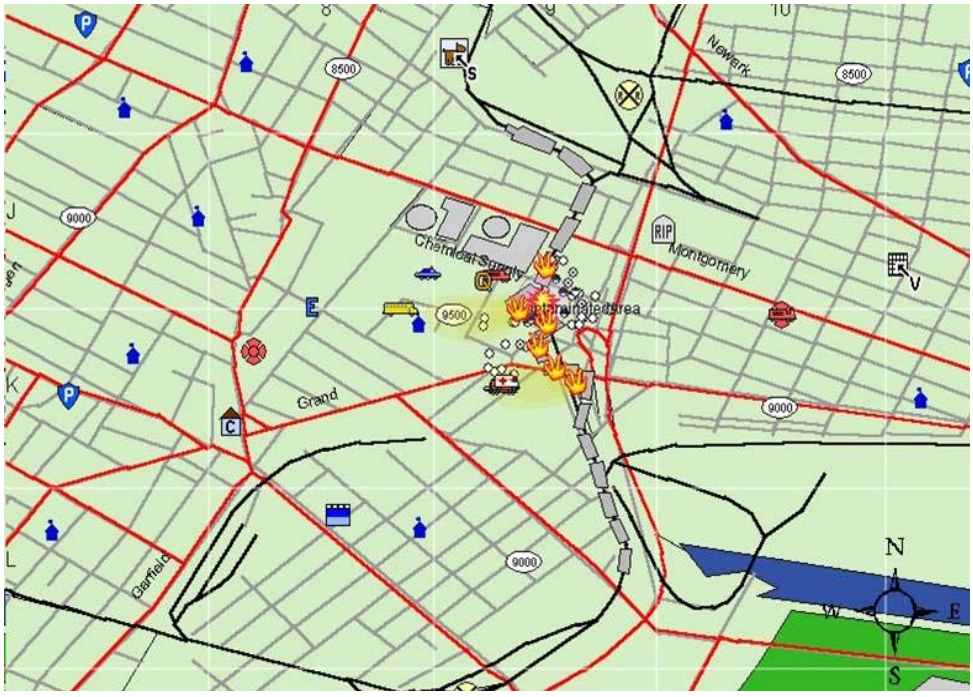

Figure 27. AEAS Map

As shown above in Figure 27, (NGB, AEAS Promotional Brief, 2003, p. 8) AEAS is a PC based simulation that allows for real time collaboration between up to 20 participants through a LAN and can be set up to run within one room or between rooms, depending upon how the local jurisdiction normally operates. The AEAS provides each participant with scenario information and provides situational message traffic, according to the role that participant is playing. The AEAS scenario map details the incident and the response, as well as the community's assets and how the environment changes with time within the scenario and according to the participant's response. Each participant's actions are recorded and continuous feedback is provided throughout the exercise and following the exercise in a detailed After Action Review (AAR). This AAR provides a detailed event log and compares reactions by the participants to national standards to determine areas of needed improvement. AEAS has three specific phases, pre-exercise, exercise and post exercise.

In the pre-exercise, the local jurisdiction is able to build out the scenario with real time information specific to the assets available in their jurisdiction and plot that information against either a provided map or against a map developed from satellite imagery. This data consists of information such as police, firefighting and medical assets and their locations to include equipment types. Once completed, this phase provides a fairly accurate depiction of what the response communities have to work with in a disaster. During this phase, the role players are selected from their areas of responsibility within the response to include all levels up to and including the National Guard liaison. Some examples of the positions would be that of incident commander, administration, law enforcement, public affairs, chaplaincy, HAZMAT, medical support and military support. There are 37 possible roles that could be played in the next phase.

In the exercise phase, the participants are faced with one of the following scenarios:

1. Anti abortion, domestic anthrax hoax
2. Anti-government, domestic anthrax contamination

3. Retribution, foreign group radiological

4. Domestic group sarin, public outdoor

5. White supremacist domestic, phosgene/propane derailment

6. Disgruntled individuals, foot and mouth several farms

7. Retribution, foreign group conventional explosive

8. Retribution, foreign group radiological, outdoor event

9. Retribution, foreign group, anthrax line source

10. Military diversion, state sponsored smallpox

11. Retribution, foreign group radiological, downtown

According to a tri-fold informational packet distributed with AEAS, the exercise phase is:

> …based on a comprehensive set of Tasks, Conditions and Standards that have been identified by stakeholder response agencies from across the nation. AEAS presents events and information on the course of the incident; receives real time input from the exercise participants, reflecting their decisions and actions; determines the results and consequences of those decisions and actions and presents the next step in the course of events based on those results and consequences. The flow of incident command ascendancy is automatically incorporated into the exercise. The system tracks players' responses and provides a real time assessment of their expected actions. (NGB, AEAS tri-fold, 2003, p. 1)

The final phase in AEAS is the post exercise phase. During this phase, the information collected in the exercise phase is provided in the form of general feedback on the status of the incident and the adequacy of the response. A diary of events shows the response of all participants as well as the consequences of those responses, to include linkages to other actions. Finally, the post exercise AAR provides an overview of how well the participants performed measured against what would be an expected effective response for that scenario.

THIS PAGE INTENTIONALLY LEFT BLANK

VII. CONCLUSION

Within the United States, incident response is a tiered system. Initial response is a local responsibility as local first responders, fire, police and medical professionals react to an event and provide assistance and analysis. This would be considered tier one as depicted in Figure 31. If the incident exceeds the capabilities of the local first response community, they enact mutual aid agreements in order to secure assistance from bordering municipalities and the state. The state's response at an incident is under the direct control of the Governor and as shown in Figure 28, (FM 3.11-22, 2003, p. 38) is tier two of the incident response. In the most serious of events, the federal government will become involved, to include the FBI and the Combatant Commander (COCOM).

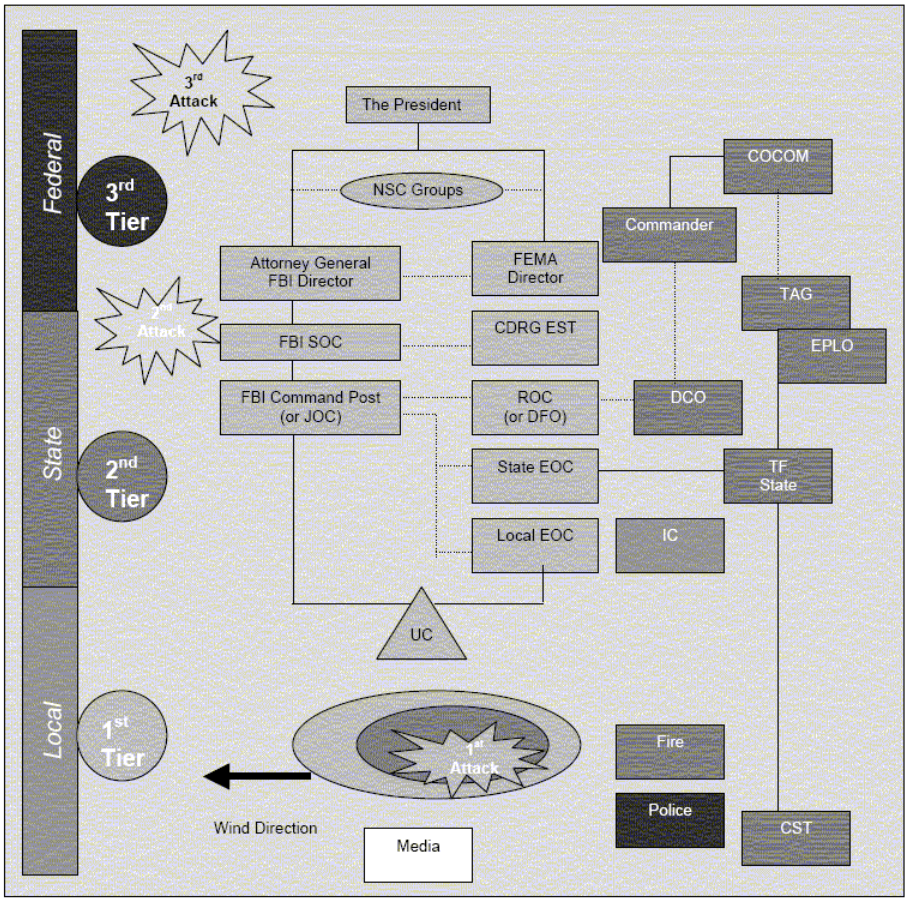

Figure 28. Tiered Response

Tier three, the third and final tier requires the most coordination of effort in order to maximize the effectiveness of the response and is governed by the Federal Response Plan (FRP). As shown, the CST is an asset the Governor can and will employ at tier one. Through the unique structure and mission of the National Guard, the CST can then continue to operate if required at tier two and finally at tier three.

Today, within the United States homeland, there exists a divide between what a local municipality can do for itself and what they entrust to government agencies. Most Americans are at least a little discomforted to see a response required by the federal component of our Armed forces. These forces have developed into units that are utilized elsewhere within the world to secure the United States and its interests. Conversely, it is common for a Governor to call out their National Guard in response to a local disaster or emergency. The community is familiar with the National Guard. It is made up of local citizens who live and work in the community. This unique role gives the National Guard a distinct advantage in the early hours after a response to bridge existing gaps between the multiple levels of response required.

In June of 2004, the member nations of the G8 held a summit hosted by the United States at Sea Island Georgia. This event framed an efficient construct of how a single military command can direct both federal and state assets. This Joint Task Force (JTF) was commanded by the Adjutant General of the State of Georgia under Title 32 status. Figure 29 (NGB, J3 DO ARNG-ANG-CNGB G8 Brief, 2004, p. 34) illustrates the lines of command and coordination for this unique situation. The Memorandum of Understanding (MOU) signed by the President and the Governor lays out the relationships very well. It states:

> The dual status commander will receive orders from a federal chain of command and a state chain of command. As such, the dual status commander is an intermediate link in two distinct, separate chains of command flowing through different sovereigns. While the dual status commander may receive orders from two chains of command, those chains of command must recognize and respect the dual status commander's duty to exercise all authority in a completely mutually exclusive manner, i.e., either in a federal or

state capacity, but never in both capacities at the same time. (NGB, MOU Concerning Use of Dual Status Commander for G8 Support Mission, 2004, p. 1)

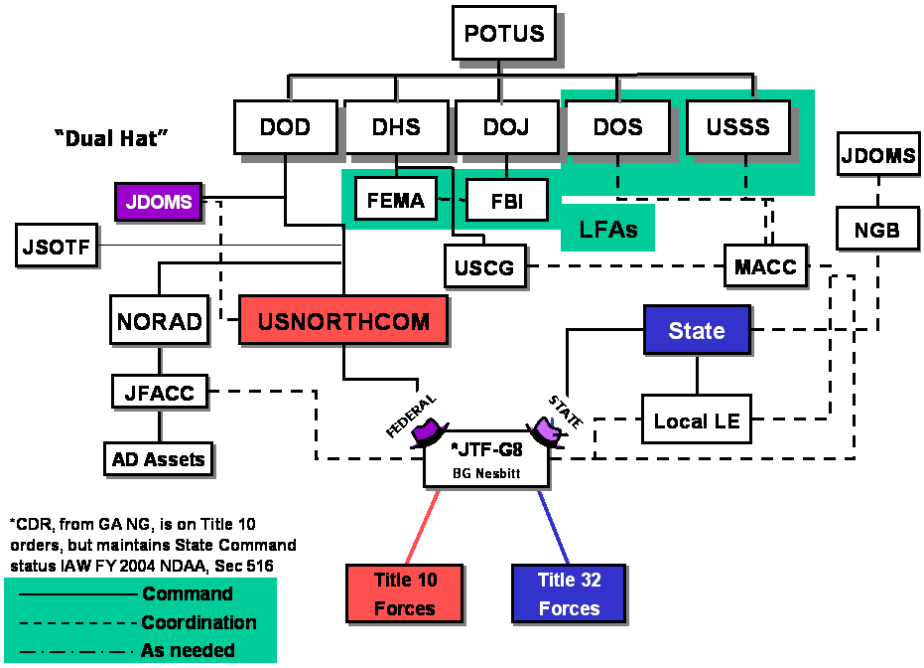

Figure 29. G8 C2 Structure

This unique command relationship is further codified in the MOU as it lays out the relationships between the state, USNORTHCOM and the JTF commander. Regarding state command and control it states:

> The Georgia Governor, through his Adjutant General, will provide command and control over the supporting National Guard forces. As a member of the Georgia National Guard in state status, the dual status commander takes orders from the Governor through the Adjutant General or the State of Georgia. The dual status commander, acting pursuant to state authority, may issue orders to National Guard forces serving in state status (Title 32 or State Active Duty). (NGB, MOU Concerning Use of Dual Status Commander for G8 Support Mission, 2004, p. 1)

Regarding the federal role of the same dual status commander, the MOU states:

> CDRUSNORTHCOM will provide command and control over the supporting federal forces. The dual status commander, as a federal officer activated under Title 10 (of the U.S. Code), takes orders from the President or those federal officers the President and Secretary of Defense have ordered to act on their behalf. The

> dual status commander, acting pursuant to federal authority, may issue orders to federal forces, i.e. active duty forces and activated reserve forces (including federalized National Guard forces). Law enforcement activities are not to be performed by federal forces in support of the G8 in violation of the Posse Comitatus Act. (NGB, MOU Concerning Use of Dual Status Commander for G8 Support Mission, 2004, p. 2)

Placing the JTF under the command of a dual status commander, a National Guard Adjutant General, highlights the dual nature of the National Guard. The MOU highlights the benefits of utilizing the National Guard in this way. It states:

> Utilizing a dual status commander allows the efficient use of both federal and state authorities to execute authorized missions in support of federal agencies for the G8 Summit. This relationship will capitalize on military expertise of both sovereign military forces, reduce duplicative effort, provide synergy, and ensure unity of command. The dual status commander will have enhanced situational awareness through this dual status, and both federal and state chains of command will have a common operating picture. (NGB, MOU Concerning Use of Dual Status Commander for G8 Support Mission, 2004, p. 2)

The JTF operation in support of the G8 mission by all accounts was a success. This type of dual status relationship is sure to be repeated as it flows logically from the complex relationship between the states and territories and the federal government. If resourced and given the mission, the National Guard CST team has the legal authority and the foundational equipment to bridge both the technology divide and the divide in authority lines between the local, state and federal agencies charged with incident response and consequence management. Given the manpower and the equipment to augment the current mission of the CST communications section, the National Guard CST teams could begin to bridge the divide between the disparate FM, UHF, satellite and data networks. It is through pilot programs and demonstrations such as NEDIS, the extended range WLAN, ESRI Notifier and AEAS that the National Guard CST communications capability could be exercised and woven into the way our nation responds to a crisis. This on-scene communications capability, tied together with the multiple operations centers and networks through a construct such as the

JCCSE, could provide the information technology support required for the dual status commander and his or her dual chains of command.

Once the decision has been made to implement JCCSE, a structured engineering process should be undertaken for the development of the physical system. As illustrated by this thesis, the requirements and interfaces for any one national IT response system are extremely complex and functional needs must be accurately identified to support early iterations of design. According to Blanchard and Fabrycky the traditional engineering design methods:

> …are based on a bottoms-up approach. Starting with a known set of elements, design engineers create a product or system by synthesizing a combination of system elements. However, it is unlikely that the functional need will be met on the first attempt unless the system is simple. (Blanchard and Fabrycky, 1998, p. 28)

In contrast, according to Blanchard and Fabrycky, the systems engineering approach is a more directed methodology which is based on:

> …a top down approach to design. Starting with the requirements about the external behavior of any part of the system (expressed in terms of the function provided by that part), that behavior is analyzed to identify its functional characteristics. These functional behaviors are then described in more detail and made specific through refinement. Finally the appropriateness of this choice of functional components is verified by synthesizing the original part. (Blanchard and Fabrycky, 1998, p. 28)

Figure 30 (Blanchard and Fabrycky, 1998, p. 27) illustrates quite well the systems engineering process.

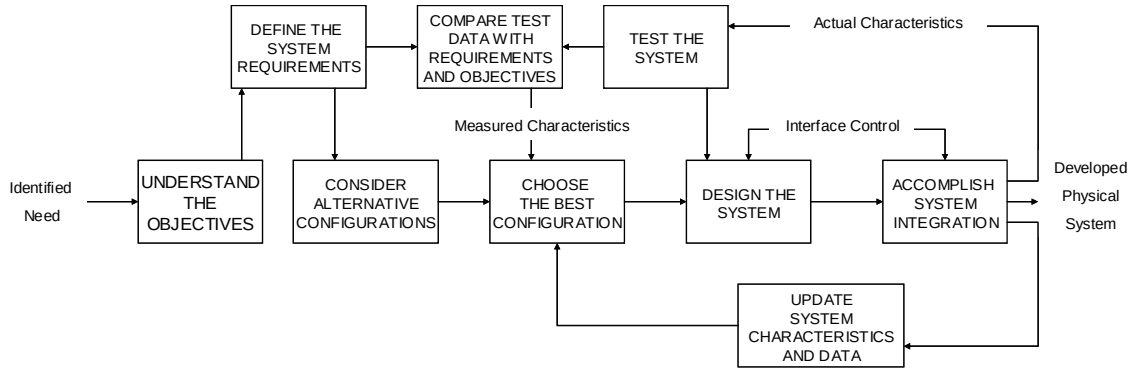

Figure 30: Systems Engineering Process

Figure 30 demonstrates how first the team must understand the objectives as defined by the identified need. In this thesis, there are a number of identified needs at all tiers of the incident response structure. These needs can be categorized broadly as types of vertical and horizontal communication. Once the objectives are understood, perhaps the single most important aspect of the process begins. This aspect is requirements definition. Although not shown in Figure 30, it is essential that this step be revisited throughout the process to continually refine the requirements. This process should be supported through the Integrated Product Team (IPT) process, with the IPT being made up of representatives from the many requirements owners and members of the design team. Once the requirements are defined, metrics are identified to measure your system against those requirements and then design, testing and integration begin.

Due to the complexity and size of the JCCSE system, a mixed engineering approach utilizing both methodologies would result in the most efficient design. Since this construct is so large and complex, the systems engineering approach should be utilized to partition JCCSE into its elements. An example of one JCCSE element is the incident response communication element. Once the construct is broken down into its elements, the bottom up design can be utilized

to capitalize on existing infrastructure to synthesize products to meet the functional requirements of that element. These elements can then be combined into the overall JCCSE.

As the United States prepares itself for the inevitable, the next terrorist incident, it becomes essential that those charged with protecting our country have a common operating picture. Through multiple simulations run in different localities, the concept of providing that common operating picture at the highest levels can be demonstrated and the lessons learned can be utilized to begin intelligence fusion within the various operations centers. It is apparent that the information is available, but through divides created both by technology and technique, that information is either lost or clouded in delivery. If America is to be effective in fighting terrorism at home and abroad, it is essential that we give our decision makers the tools and accurate information required to make timely and effective decisions.

THIS PAGE INTENTIONALLY LEFT BLANK

VIII. RECOMMENDATIONS FOR FURTHER STUDY

This thesis has shown some of the many areas that must be addressed if the United States is to bridge the incident response digital divide. It is as important that those who decide the course our country takes in its response to disaster have an accurate picture of how we respond today as it is for those actually responding to have an accurate picture of what situation exists and what assets are available. It is recommended that the National Guard be utilized as envisioned by our forefathers to defend and secure the homeland, and that it be resourced appropriately. There are many initiatives underway that begin to build on our strengths as a nation and that expose our weaknesses. The data in this thesis demonstrates the current capabilities existing within the United States for incident response at the local, state and federal levels. Further study should be given to identify those specific gaps that exist between our current capabilities and our desired end state.

It is recommended that further study be given to the following areas:

1. Analysis of the redundancies in the EOC systems
2. Bridging the communications gap at the incident site
3. Bridging the communications gap at the EOC level and higher
4. Information mining and knowledge management in support of incident response

An in depth analysis of the EOC communications systems would expose many redundancies and additional touch points that could be leveraged to minimize the cost of bridging the response systems together. Many of those redundancies could be targeted for elimination, though an understanding of what consequences would occur due to those eliminations must occur prior to any action. It is important to note that some redundancy is required in order to provide continuity of operations should critical infrastructure be targeted.

It is recommended that additional study be given to identifying the communications gaps at the incident site. It is critical to understand how the fiscal and policy decisions that are made exacerbate that gap. Some of the communications gaps will be due to interoperability problems between the different response networks caused by technology and some will be caused by policy. Both of these need further study and an in-depth gap analysis.

Throughout the United States there are thousands of networks and hundreds of agencies that are charged with homeland defense and homeland security. It is recommended that further study be given to how we can bridge the communications gap at the EOC level and higher to efficiently manage resources and provide the incident commander with the appropriate mix of response at the appropriate time and at the appropriate place. Many localities have established mutual aid pacts that speed response from their neighboring towns and counties, but this model does not efficiently extend beyond the state borders in the event a national response is required.

Having information and the ability to deliver it is important, however lacking the understanding of what the information really represents makes all of the effort to gather and deliver it moot. It is recommended that further study be given to how we can mine the information from the incident site and the EOC and bridge the communications gap in order to provide a common operating picture at all levels of government, from the Governor to the President, in order to have an understanding of the entire scenario that may be unfolding. In this way the graduated response can be properly applied strategically in order to avoid critical shortages and or delays in implementation that will certainly cost human lives.

This thesis' final recommendation is that an in depth demonstration or pilot be undertaken where two way data flow be achieved from multiple incident sites to the local EOC, the state EOC and JFHQ State JOC, the NGB JOC, the USNORTHCOM and USPACOM JOCs and the Homeland Security operations center. That pilot should demonstrate the JCCSE concept and more importantly, demonstrate the ability to fuse information and intelligence from disparate

sources. It should implement the accepted response plans at all levels and should be measured against pre-defined metrics that demonstrate our strengths and weaknesses when we respond as a nation to a threat within our own borders.

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF REFERENCES

1. Blanchard, Benjamin S. and Fabrycky, Wolter J. (1998) *Systems Engineering and Analysis,* 3d ed. New Jersey: Prentice-Hall

2. Blum, Steven H. LTG (2003) *CNGB Joint IT Conference Speech*, (2003) National Guard Bureau (Document stored locally, contact Sharon Lenius: sharon.lenius@ngbcio.ngb.army.mil)

3. Blum, Steven H. LTG (2004) *Statement by LTG H Steven Blum, Chief, National Guard Bureau before the Subcommittee on Terrorism, Unconventional Threats and Capabilities Committee on Armed Services, United States House of Representatives* (Document stored locally, contact Sharon Lenius: sharon.lenius@ngbcio.ngb.army.mil)

4. Cavil, Michael P. (2002) *Analysis of the Department of Defense Homeland Security Support Organization,* Master's Thesis, Monterey, CA. The Naval Postgraduate School

5. Dennis, Lathan (2004) *Fairfax County Community Services Board Emergency Response System: Notifier*, retrieved June 3, 2004 from http://www.directionsmag.com/article.php?article_id=468

6. Department of Homeland Security (2003) *DHS JRIES Brief* (Document stored locally, contact Sharon Lenius: sharon.lenius@ngbcio.ngb.army.mil)

7. Department of Homeland Security (2004a) *DHS Organization Brief* retrieved May 17 2004 from www.dhs.gov

8. Department of Homeland Security (2004b) *DHS PEP Equipment Location Brief* (Document stored locally, contact Sharon Lenius: sharon.lenius@ngbcio.ngb.army.mil)

9. *Department of Homeland Security Organization* (2004) retrieved May 14, 2004 from http://www.dhs.gov/dhspublic/display?theme=9&content=2973

10. *DISN Information Sheet*, (2004) retrieved June 10, 2004 from http://www.disa.mil/main/prodsol/data.html#nipr

11. Eberhart, Ralph E. General (2003) *Testimony by General Eberhart before the House Armed Services Committee* retrieved June 10, 2004 from http://www.norad.mil/index.cfm?fuseaction=home.news_rel_03_31_04

12. *FM 3.11-22* (2003) retrieved June 1, 2004 from http://www.army.mil/usapa/doctrine/Browse_Series_Collection_1.html

13. *GAO Report, Homeland Security IT Funding and Management Issues, GAO-03-250* (2002) retrieved July 7 2004 from http://www.gao.gov/new.items/d03250.pdf

14. *GAO Report, Homeland Security, Efforts to Improve Information Sharing Need to be Strengthened, GAO-03-760* (2003) retrieved July 7 2004 from http://www.gao.gov/new.items/d03760.pdf

15. *GAO Report, Project SAFECOM, GAO-04-494* (2004) retrieved July 7, 2004 from http://www.gao.gov/new.items/d04494.pdf

16. *HSIN Fact Sheet* (2004) retrieved June 1, 2004 from http://www.dhs.gov/dhspublic/display?content=3648

17. *Iowa Fact Sheet* (2004) retrieved June 1, 2004 from http://www.iowanationalguard.com/

18. Legal Information Institute (2004) *US Code Collection* retrieved August 17, 2004 from http://www4.law.cornell.edu/uscode/18/1385.html

19. Lockwood, Edward W. (2003) *The Changing Role of the Army National Guard,* Master's Thesis, Monterey, CA. Naval Postgraduate School

20. National Guard Bureau (2003) *AEAS Fact Sheet* (Document stored locally, contact Sharon Lenius: sharon.lenius@ngbcio.ngb.army.mil)

21. National Guard Bureau (2003) *AEAS Promotional Brief* (Document stored locally, contact Sharon Lenius: sharon.lenius@ngbcio.ngb.army.mil)

22. National Guard Bureau (2003) *AEAS Tri-fold* (Document stored locally, contact Sharon Lenius: sharon.lenius@ngbcio.ngb.army.mil)

23. National Guard Bureau (2003) *ANG Enterprise Network Architecture Profile* (Document stored locally, contact Sharon Lenius: sharon.lenius@ngbcio.ngb.army.mil)

24. National Guard Bureau (2003) *Annex D JFHQST Transformational Guidance Organization Charts* (Document stored locally, contact Sharon Lenius: sharon.lenius@ngbcio.ngb.army.mil)

25. National Guard Bureau (2003) *Army Knowledge Symposium Brief* (Document stored locally, contact Sharon Lenius: sharon.lenius@ngbcio.ngb.army.mil)

26. National Guard Bureau (2004) *DTTP Shared Usage Brief* (Document stored locally, contact Sharon Lenius: sharon.lenius@ngbcio.ngb.army.mil)

27. National Guard Bureau (2003) *Guard AEI Initial Implementation Project Brief* (Document stored locally, contact Sharon Lenius: sharon.lenius@ngbcio.ngb.army.mil)

28. National Guard Bureau (2001) *JettCon Shared Usage Brief* (Document stored locally, contact Sharon Lenius: sharon.lenius@ngbcio.ngb.army.mil)

29. National Guard Bureau (2004) *JCCSE Point Paper* (Document stored locally, contact Sharon Lenius: sharon.lenius@ngbcio.ngb.army.mil)

30. National Guard Bureau (2003) *JFHQST Transformational Guidance* (Document stored locally, contact Sharon Lenius: sharon.lenius@ngbcio.ngb.army.mil)

31. National Guard Bureau (2004) *J3 Conference Brief* (Document stored locally, contact Sharon Lenius: sharon.lenius@ngbcio.ngb.army.mil)

32. National Guard Bureau (2004) *J3 DO ARNG-ANG-CNGB G8 Brief* (Document stored locally, contact Sharon Lenius: sharon.lenius@ngbcio.ngb.army.mil)

33. National Guard Bureau (2004) *MOU Concerning Use of Dual Status Commander for G8 Support Mission* (Document stored locally, contact Sharon Lenius: sharon.lenius@ngbcio.ngb.army.mil)

34. National Guard Bureau (2003) *NGB BRIEF Kickoff* (Document stored locally, contact Sharon Lenius: sharon.lenius@ngbcio.ngb.army.mil)

35. National Guard Bureau (2002) *NGB IT Brief to the United Kingdom ADL Partnership Lab (*Document stored locally, contact Sharon Lenius: sharon.lenius@ngbcio.ngb.army.mil)

36. National Guard Bureau (2004) *NGB IT Vision/Mission Brief* (Document stored locally, contact Sharon Lenius: sharon.lenius@ngbcio.ngb.army.mil)

37. National Guard Bureau (2004) *NGB J3 NEDIS Brief* (Document stored locally, contact Sharon Lenius: sharon.lenius@ngbcio.ngb.army.mil)

38. National Guard Bureau (2004) *NGvision Brief* (Document stored locally, contact Sharon Lenius: sharon.lenius@ngbcio.ngb.army.mil)

39. National Guard Bureau (2004) *2005 National Guard Posture Statement* (Document stored locally, contact Sharon Lenius: sharon.lenius@ngbcio.ngb.army.mil)

40. Northrop Grumman Inc. (2004) *Wireless LAN in Public Safety 802.11b* (Document stored locally, contact Sharon Lenius: sharon.lenius@ngbcio.ngb.army.mil)

41. Office of Domestic Preparedness (2004a) *Agency PEP Brief* (Document stored locally, contact Sharon Lenius: sharon.lenius@ngbcio.ngb.army.mil)

42. Office of Domestic Preparedness (2004b) *PEP Equipment Set* (Document stored locally, contact Sharon Lenius: sharon.lenius@ngbcio.ngb.army.mil)

43. RCAS Summary (2003) retrieved June 03, 2004 from http://www.rcas.com/rcas_summary.htm

44. Scott, Gerald R. (2003) *Bureaucracies, Communities and Networks: Interagency Cooperation for Homeland Security in Monterey County*, Master's Thesis, Monterey, CA. The Naval Postgraduate School

45. Sullivan, Paul. (2004a) *CST UCS vs DRS C3V Comparison* (Document stored locally, contact Sharon Lenius: sharon.lenius@ngbcio.ngb.army.mil)

46. Sullivan, Paul. (2004b) *NGB DP04 Informational Spreadsheet* (Document stored locally, contact Sharon Lenius: sharon.lenius@ngbcio.ngb.army.mil)

47. Sullivan, Paul. Major General (2004) *Joint Staff Update Memorandum* (Document stored locally, contact Sharon Lenius: sharon.lenius@ngbcio.ngb.army.mil)

48. Under Secretary of Defense for Strategy and Threat Reduction (2004) *RCES Reserve Component Employment 2005 Study Report* (Document stored locally, contact Sharon Lenius: sharon.lenius@ngbcio.ngb.army.mil)

49. United States Constitution Article I, Section 8 (2004) retrieved August 20, 2004 from http://www.house.gov/Constitution/Constitution.html

50. United States Northern Command (2004) *USNORTHCOM Concept of Operations* (Document stored locally, contact Sharon Lenius: sharon.lenius@ngbcio.ngb.army.mil)

51. Van Fleet, Frank C. *The Foundation and Development of the National Guard Bureau*, (2002) NGB Primer, Minute Man Institute for National Defense Studies

52. Walsh, Mark C. (1991) *Free Men Shall Stand*, Oxford Press, New York, NY: Oxford University Press

THIS PAGE INTENTIONALLY LEFT BLANK

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California

3. Ms. Maureen Lischke, NGB Deputy J6
   National Guard Bureau
   Arlington, Virginia